



Protection Studio

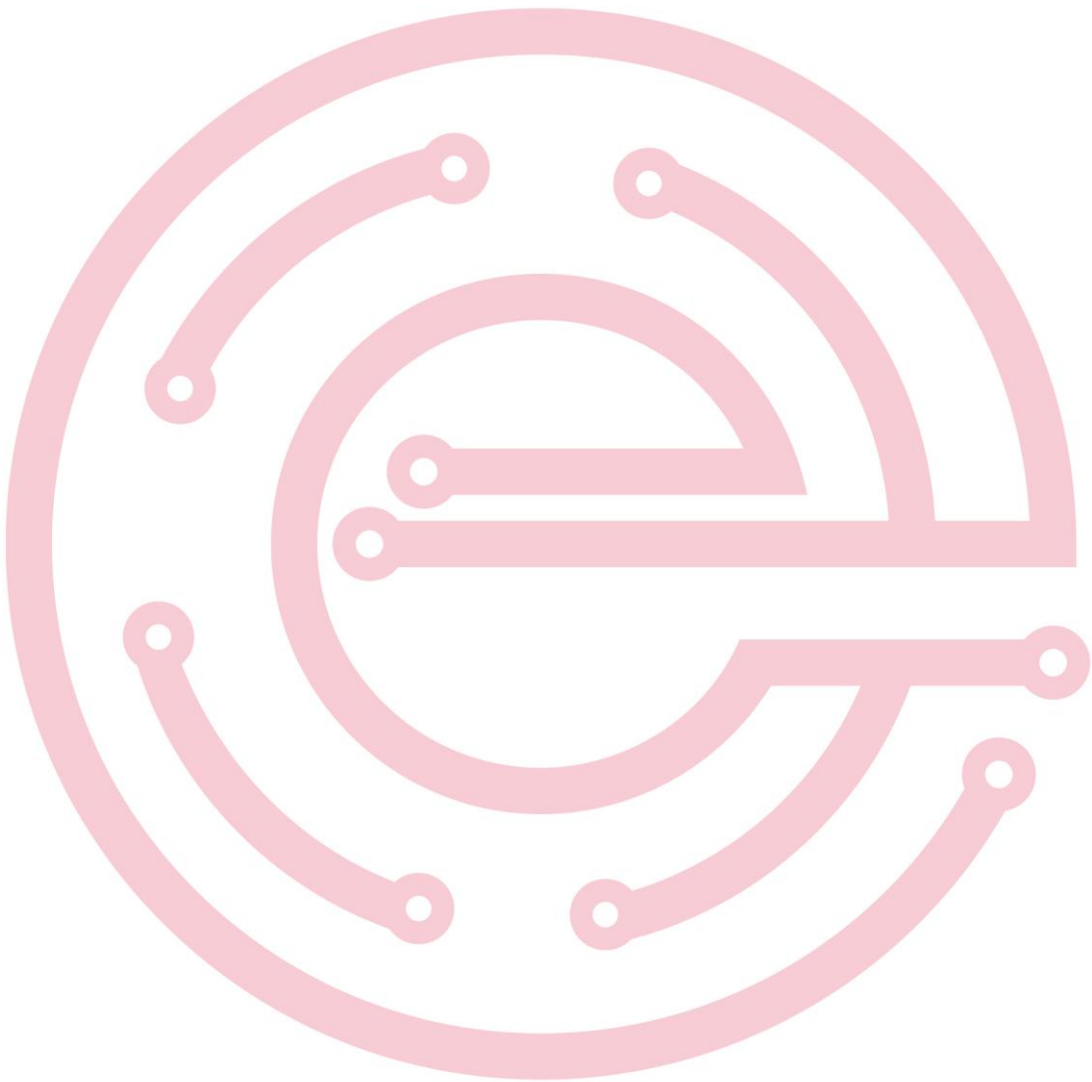


I. CONTENTS

II. INTRODUCTION	4
OVERVIEW	4
COPYRIGHTS AND TRADEMARKS	4
III. E-CODE PROTECTION STUDIO V5.3.4	5
INTRODUCTION	5
E-CODE PROTECTION STUDIO PROCESS	6
SOFTWARE PROTECTION LAYERS	7
<i>License Management Layer</i>	7
<i>SDK Layer</i>	8
<i>SHELL Protection Layer</i>	8
<i>Cryptographic Layer</i>	9
<i>Hardware Layer</i>	9
IV. FEATURES	10
PROTECTION STUDIO ACTIVATION	10
PROTECTION STUDIO SETTINGS	10
VENDOR PROFILES	11
PROTECTION TITLES	12
<i>Software and Data Title</i>	12
<i>Data Only Title</i>	12
<i>Test Mode Title</i>	12
<i>Final Mode Title</i>	12
LICENSE DESCRIPTION	14
<i>General License Attributes</i>	14
<i>License Modules</i>	16
EXECUTABLE PROTECTION	18
<i>Protection Levels</i>	18
<i>Customized Protection Solutions</i>	19
DATA FILES ENCRYPTION	20
<i>Data Protection for R/W Files</i>	20
SAFE CD PROTECTION	20
<i>CD STD</i>	21
<i>CD PRO</i>	22
SAFE CDR PROTECTION	23
<i>Technology</i>	23
<i>Characteristics</i>	23

<i>Process</i>	23
SAFE KEY PROTECTION	24
<i>Technology</i>	24
<i>Characteristics</i>	24
<i>Process</i>	24
SAFE ACTIVATION PROTECTION	25
<i>Technology</i>	25
<i>Characteristics</i>	25
<i>Process</i>	25
SOFTWARE PROTECTION MODELS	27
<i>Safe Shell</i>	27
<i>Safe Key with Single License and Single Key</i>	28
<i>Safe Key with Single License and Multiple Keys</i>	29
<i>Safe Key with Multiple License and Single Key</i>	30
<i>Safe Key with Run on First Machine</i>	31
SOFTWARE LICENSING MODELS	33
<i>Trial License</i>	33
<i>Rental License</i>	34
<i>Features License</i>	35
<i>Network License</i>	36
<i>Network/Portable License (Hybrid)</i>	37
LICENSE UPDATE	42
<i>Safe Key License Update</i>	42
<i>Safe Activation License Update</i>	43
<i>Protection Techniques Migration</i>	45
OFFLINE ACTIVATION (PHONE)	47
<i>Safe CD with Offline Activation</i>	47
<i>Safe Activation with Offline Activation</i>	48
DATA ONLY PROTECTION	50
PROTECTION WITH SDK	51
V. PROTECTION SAMPLES	55
SAFE CD/CDR SAMPLE	55
SAFE ACTIVATION SAMPLE	56
SAFE KEY SAMPLE	58
VI. SPECIFICATIONS	59
E-CODE PROTECTION STUDIO V5.3.4	59
SAFE CD/CDR	59

SAFE KEY	60
SAFE ACTIVATION.....	60
I. ABOUT E-CODE	61



II. INTRODUCTION

This document provides a Product Description for the E-Code Protection Studio. The product description covers the different features and techniques of E-Code Protection Studio v5.3.4. The product description will provide a complete view for software vendors on how to make a good use of E-Code Protection Studio v5.3.4 in a way that meets their software protection and distribution requirements.

Overview

E-Code Protection Studio v5.3.4 is the new product version of E-Code software protection solution line of products. E-Code Protection Studio v5.3.4 is a software tool that provides to software vendors advanced and various techniques to protect their software against Reverse Engineering, Piracy and Illegal distribution.

E-Code Protection Studio v5.3.4 provides All in One software protection tool. The Protection Studio provides different protection techniques in a single tool. Protection techniques vary to meet the software vendors' needs. Protection techniques include:

1. CD/DVD Protection
2. CDR Protection
3. USB Dongle Protection
4. Online Activation Protection

All techniques are combined with advanced software protection (Shell Protection) that protects the software source code and data. In addition, E-Code Protection Studio v5.3.4 provides a flexible and advanced SDK for extending the software security to be within the hands of the developer.

E-Code Protection Studio v5.3.4 introduces a new and advanced License Management System that meets different requirements to control the Condition and Rights for the sake of software security and distribution.

Copyrights and Trademarks

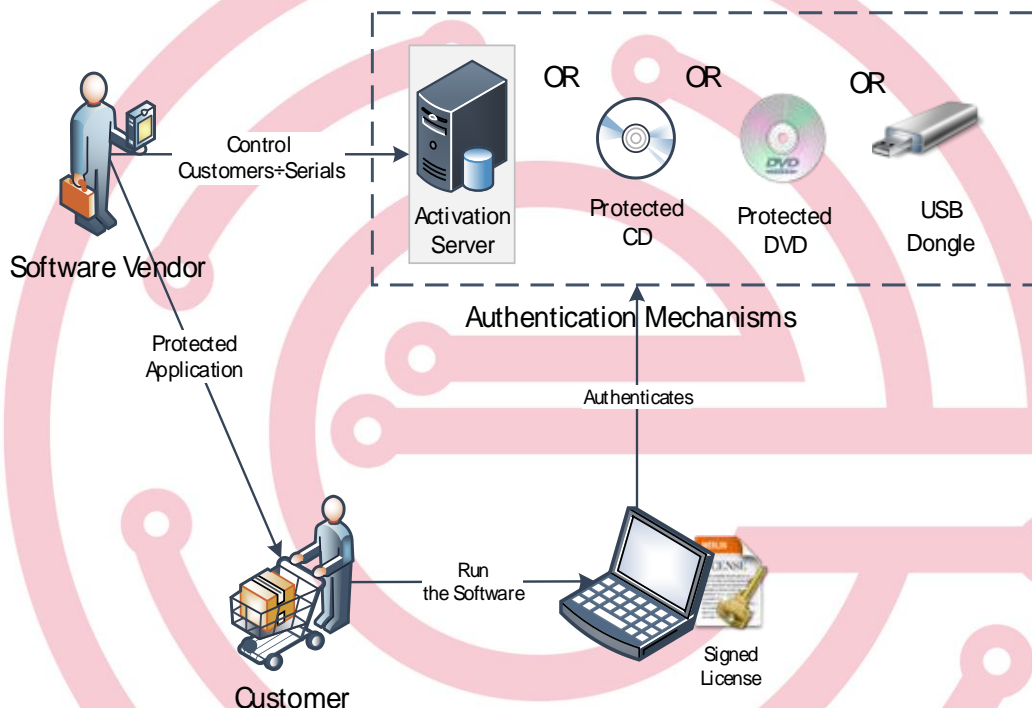
All of the content on this manual and accompanying software(including all text, graphics, sounds, demos, patches, hints and other files) is covered under KSA and international copyright and trademark laws by E-Code and other companies, and are property of E-Code, or are presented with permission and/or under license. This content may not be used for any commercial use without express written permission of E-Code, and possibly other copyright or trademark owners. All other trademarks and copyrights are the property of their respective owners.

©2015, E-Code

III. E-CODE PROTECTION STUDIO v5.3.4

Introduction

The next figure illustrates an example of a software distribution process. Where the software vendor needs to protect his intellectual property and his copyright as well. He also needs to enforce different protection conditions for each software release like trials or expiration date.



The example displays four effective techniques for the software protection via:

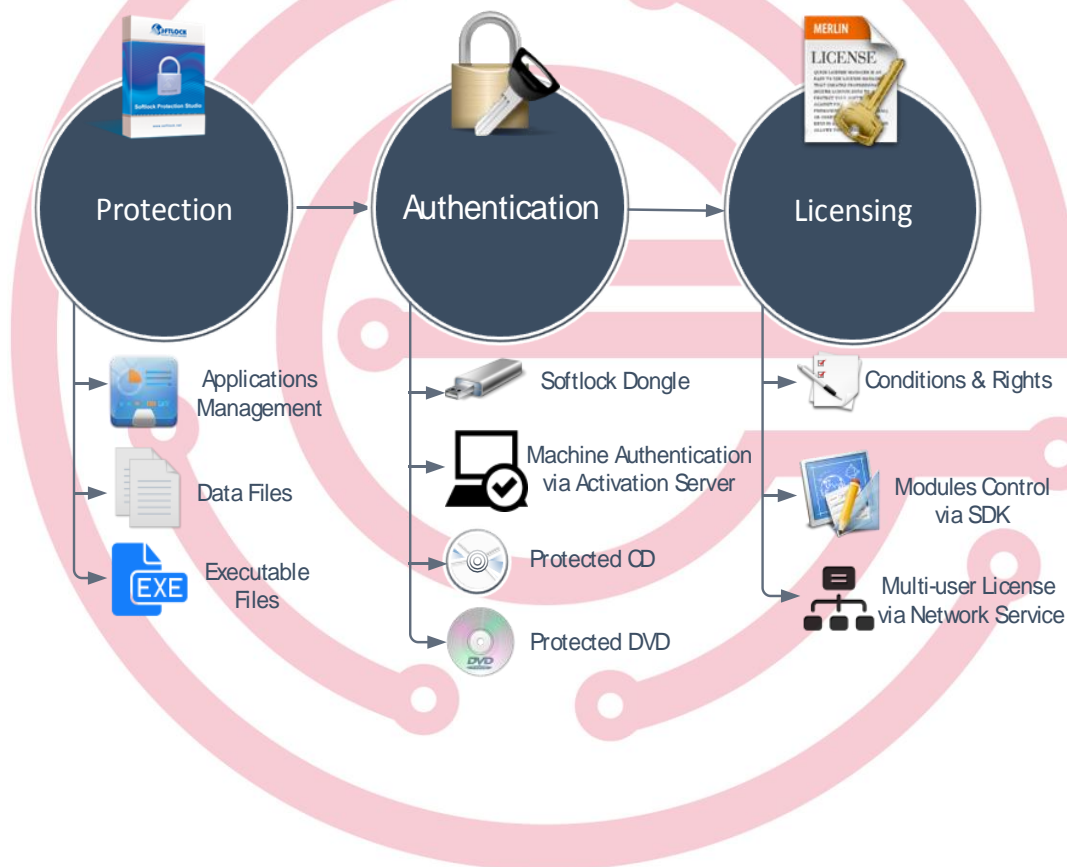
- USB Hardware authentication device.
- Machine authentication with serial numbers.
- CD authentication.
- DVD authentication.

E-Code Protection Studio Process

E-Code provides Software Protection Studio v5.3.4 to automate the software protection process. The protection is characterized as multi-layered protection that can be customized to meet the software vendor requirement. The challenging security in this solution is that it is based on hardware protection as mentioned in the previous figures, which resists all piracy operations.

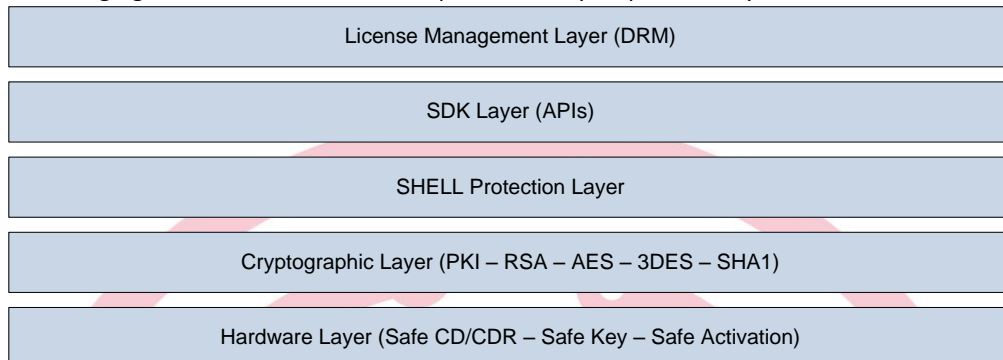
E-Code Protection process can be divided into three major stages:

1. Protection: Software Protection of executable and data files.
2. Licensing: License editing and issuing.
3. Authentication: Authentication mechanism preparation.



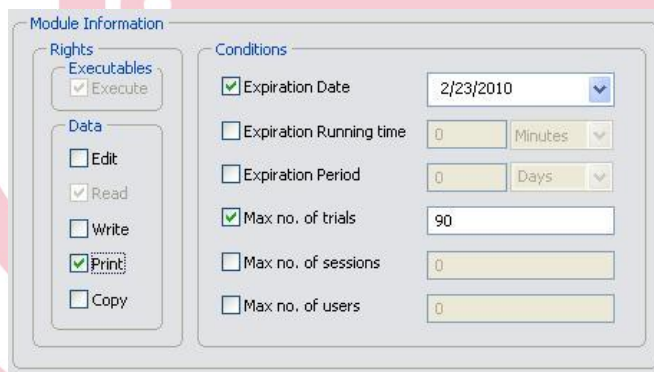
Software Protection Layers

The following figure describes the different protection layers provided by E-Code Protection Studio.



License Management Layer

License Management Layer is responsible for controlling the software DRM and distribution process. E-Code Enterprise Software Protection uses a license model based on XrML standard. The license is characterized by its readability and high security depending on PKI standards. The following screenshots are taken from E-Code Protection Studio v5.3.4 illustrating the different rights and conditions available in any license.



General

License Label: License Sequence Number:

Protection Type: ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☐ Enable SDK APIs

Authentication Type: ☐ Network License

Modules

<input checked="" type="checkbox"/>	Module Name	Module Type
<input checked="" type="checkbox"/>	Default Module	MODULE
<input checked="" type="checkbox"/>	HR. Module	MODULE
<input checked="" type="checkbox"/>	Sales Module	MODULE
<input checked="" type="checkbox"/>	Management Module	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit
☒ Read
☒ Write
☒ Print
☒ Copy

Conditions

☐ Expiration Date:

☐ Expiration Running time:

☒ Expiration Period:

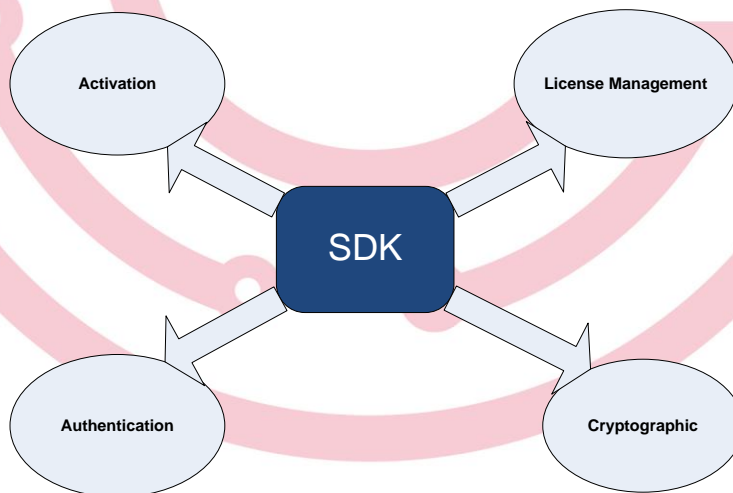
☐ Max no. of trials:

☐ Max no. of sessions:

☐ Max no. of users:

SDK Layer

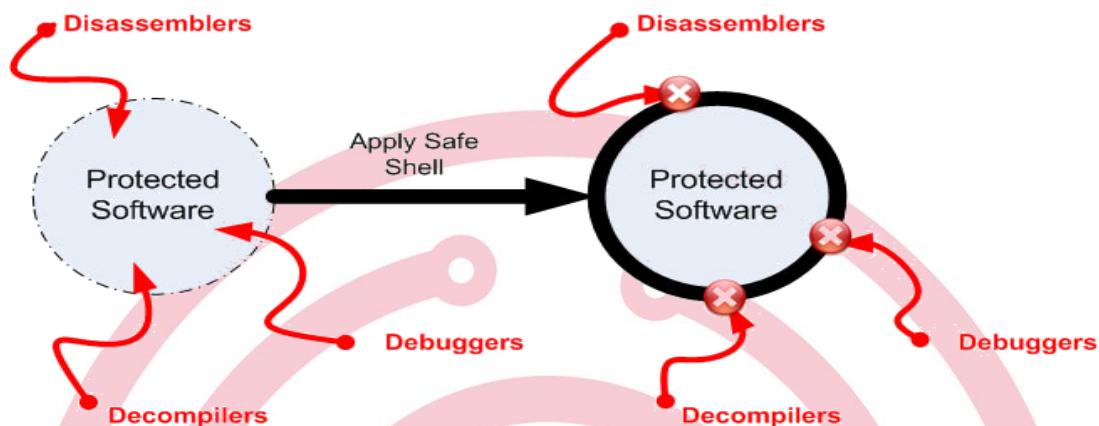
E-Code Protection Solution provides a flexible SDK giving the software vendor to integrate the software with the Security system, linking License Management System and Hardware protection devices with the written software source code. The SDK provides various APIs that give full flexibility for the developers.



SHELL Protection Layer

Shell Protection layer is a layer responsible for protecting the intellectual property of the software vendor. Shell protection simply encrypts all the source code and data in the software, and modifies

the protected file structure in order to protect the vendor Intellectual Property. Shell Protection doesn't modify the behavior of the software though it provides extra protection against software cracking and reverse engineering.



Cryptographic Layer

E-Code Software Protection Solution depends on strong cryptographic libraries and standards which adds extra strength to the system. Protecting the software source code and data with strong and trusted symmetric encryption (AES and 3DES) gives strength against decrypting the software source code. While depending on PKI certificates and RSA cryptography provides strength in combining the security with a hardware device. E-Code Protection Solution doesn't use a single key for decryption, though it uses multiple distributed keys with multi wrapping mechanisms.

Hardware Layer

E-Code Protection Solution delivers the highest level of security by combining all the mentioned layers with a hardware layer. The hardware layer provides different techniques for protecting the software against piracy and illegal distribution. Binding the software protection with a hardware device adds extra strength to system and provides the ability to resist any reverse engineering and software cracking attacks.

IV. FEATURES

E-Code Protection Studio v5.3.4 is composed of several modules, combined together to provide the full software and data security.

Protection Studio Activation

Protection Studio is activated by:

1. **Using Online Activation:** The Studio is activated here using Internet Activation and a Serial. This technique requires internet connection existence during using the Protection Studio.
2. **Using Dongle Activation:** The Studio is activated here using Dongle activation. This technique will require distributing the Protection Studio with a unique USB key used in operating the studio. This technique is suitable for vendors who are using the studio in an environment that is not connected to internet.

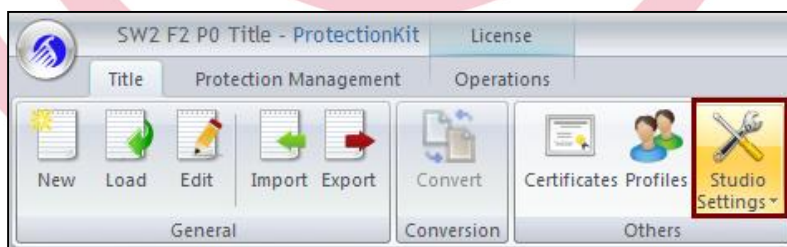
After activating the Protection Studio, any vendor can start running on the studio and can establish any kind of protection. The Protection Studio is controlled via License issued by E-Code; this license will provide the specific rights and conditions that a vendor has during operating on the studio.

Protection Studio Settings

Protection Studio settings is essential in operating on the Protection Studio. Settings include

1. **Default Paths:** Includes setting the paths of operating database, executable backup and data backup.
2. **Backup Database:** An option to back up the Operating Database.
3. **Update Studio:** A step to update the studio to the latest version.

The Operating Database is very important as it includes all protection parameters for all titles.¹



¹ The Protection Studio mainly depend on the Operating Database to store most of protection parameters and vendor's information. And the vendor takes the responsibility of preventing its deletion.

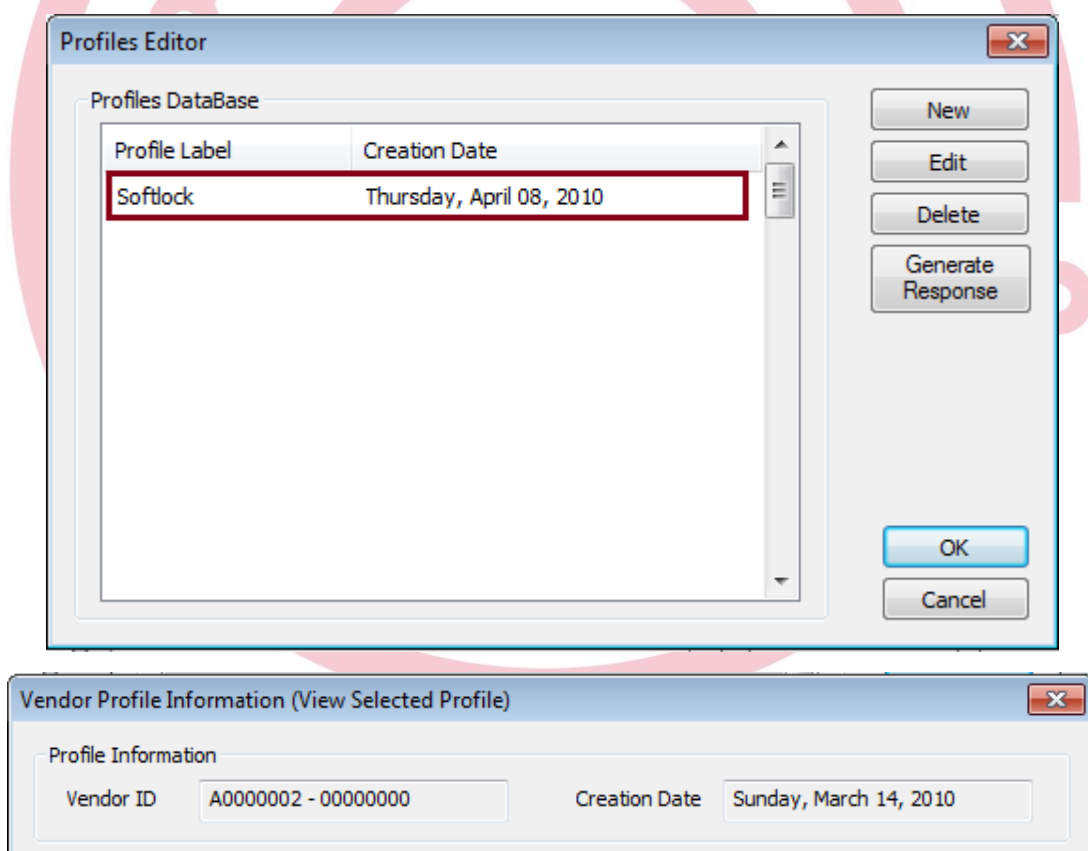
Vendor Profiles

Vendor Profile is the module that describes a vendor operating on the Protection Studio. Vendor Profile holds information about the vendor, including some descriptive information about the vendor (Name, Email, Phone ...etc.) and some data that is used in the security operation including its unique Vendor Certificate used in protection techniques.

E-Code Protection Studio v5.3.4 provides a secure and easy way to distribute the profiles to the vendors. Using Profile Request/Response method, will establish a way to deliver the profile to the studio in a secure way that cannot be used in another Protection Studio, which keeps the profile safe from misuse in unauthorized hands.

Profile request/response method is based on PKI and Hardware Certificates to secure the profile delivery operation. The profile will be used in creating Protection Titles and start the protection operations. Each vendor will have a unique Vendor ID.

The following figures illustrate the Profiles in Protection Studio.



Protection Titles

After importing a profile, creating Titles is the step to start applying protection to the software and data. Titles are used to identify specific protection project. Each title includes some information in addition to some security parameters like the protection key and Software Certificate.

Each title will be assigned a Unique Protection ID. This Protection ID will be a sequence based on the vendor ID and will describe all the protection operations within the studio. The next screen shot describes Title's parameters.

Titles can be categorized as

1. Software and Data Title
2. Data only Title

While, title protection mode can be

1. Test Mode Title
2. Final Mode Title

The mode of the title affects how the protection is applied.

Software and Data Title

This type of titles will enable the vendor to protect EXEs and Encrypt Data files within the title.

Data Only Title

This type of titles will enable the vendor to Encrypt Data file only. It will require a Viewer S/W Certificate.

Viewer S/W Certificate will be publicly available by E-Code or can be generated by the vendor. This certificate will be used by the Viewer (a protected EXE) in order to view data files encrypted under the current title.

Test Mode Title

This mode enables the vendor to apply protection techniques in test mode only. Test mode titles cannot be distributed to customers as it runs the protected EXE and Data files on the vendor machine only.

Final Mode Title

This mode enables the vendor to apply protection techniques in its final mode. It enables the vendor to distribute the software to customers as it won't be bound to vendor machine.

Protection Title Information (New Title)

General Information

Protection ID: A0000002 - 00000017 - 0000002E

Creation Date: Monday, October 18, 2010

Protection Profile: Softlock

Protection Label: CRM Project Title

Application Type: ☒ Software and Data ☐ Data Only

Protection Mode: ☒ Final Mode ☐ Test

Software Certificate: Export

Advanced Settings

Encryption Technique: AES Signature Technique: RSA

Code Length: 8

Activation Server URL: <http://www.Softlock.net/SLPSActivationServer/Process> Open

Certificate Password: ☒ Auto generated

Equations

Equation Label	

Add Remove Try

License Agreement OK Cancel

Other important properties of the title are:

1. **Encryption Technique:** The used Encryption algorithm is AES or 3DES.
2. **Code Length:** The used code length in the protection operations (ex: Machine Activation code). This property is useful in Phone Activation option. (Will be mentioned later in details)
3. **Activation Server URL:** The Activation Server URL used in Safe Activation protection.
4. **Certificate Password:** This is Auto Generated password, though it can be optionally assigned by the vendor while creating the title.
NOTE: Once the Certificate password is saved in the title, it cannot be changed.
5. **Equations:** Equations are used to add extra security for the software. (Will be mentioned later in details)

License Description

E-Code Protection Studio v5.3.4 is based on licenses. The License is a file that elaborates the rights and conditions applied on any protection. The license includes many options and attributes. One important property is that all licenses generated from Protection Studio is based on XrML standard. One benefit of conforming to standard, is that the license is readable, which gives the user the ability to read the rights and conditions supplied on the software.

The following figure illustrates the different attributes, rights and conditions of the license

The license is divided into two main parts, General and Modules:

General License Attributes

The general part of the license includes generic attributes of the license. The following are the attributes:

LICENSE LABEL

The license label will hold the label of the license. This label can be helpful when the license is distributed as it gives a descriptive property of the license.

LICENSE SEQUENCE NUMBER

The Sequence Number is a unique sequence number of the license inside each title. Once a license is issued with a sequence number, this sequence cannot be repeated in this typical title

PROTECTION TYPE

The license includes an attribute that tells what kind of hardware protection it represents. The protection type can be one of the following

1. Safe Shell
2. Safe CD/CDR
3. Safe Key
4. Safe Activation

This attribute is very important, as it represents how the protected application will operate, authenticate and activate during run-time.

ENABLE ACTIVATION BY PHONE

This is an Optional attribute, available only in Safe CD/CDR protection and Safe Activation protection. This option is very useful in case a problem happened while performing Hardware Authentication and Activation. Though, this attribute decreases the security of the protection severely.

RUN ON FIRST COMPUTER

This is an optional attribute used in Safe Key protection. The idea is to bind the Hardware key with the first machine the application runs on.

ENABLE SDK APIs

This is an optional attribute, and Should be used when the vendor is planning to use the SDK within the protected application.

AUTHENTICATION TYPE

The authentication type is a very useful attribute that can increase the security level of the protection according to software vendors' needs. The authentication types are:

1. **Once:** The application will perform hardware authentication only once. This option has low security and it is available only in Safe Activation.
2. **Once per:** The application will perform the authentication once per a period you specify.
3. **On each Startup:** The application will perform the authentication each time it runs.
4. **Periodical Check:** The application will perform the authentication according to specific time interval. This is considered the highest authentication security.

The usage of the Authentication Type attribute will be explained in details and in combination with protection techniques later.

MULTI-USER LICENSE

The Multi-user attribute is optional. It can be used when using a Network License (Explained later). This attribute may require issuing two licenses (Client and Server). This option is available in Safe Key and Safe Activation.

License Modules

The modules part is the second part of the license. Any license includes one or more modules. Each module includes set of rights and conditions. The main module is called the Default Module, which includes the main application rights and conditions. While, when adding other modules, they will hold their rights and conditions. The added module can be accessed only when using SDK.

The following are the rights and conditions in the license

RIGHTS

The rights act as DRM for the software and data

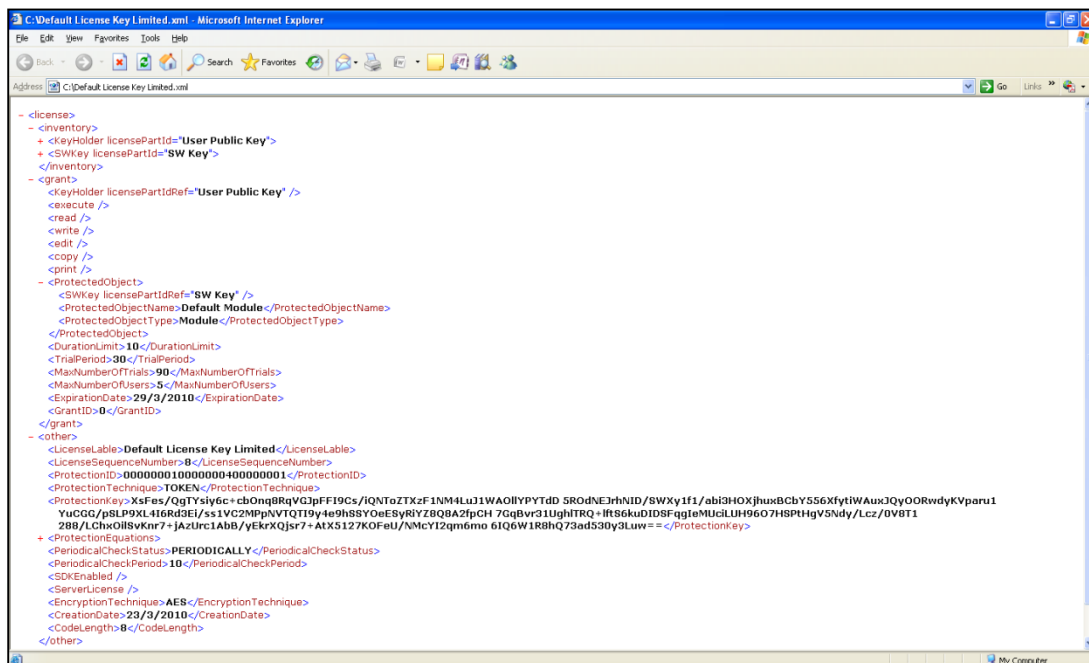
1. **Execute:** This indicates whether the module is enabled or not
2. **Read:** This indicates whether the module is enabled or not
3. **Edit:** Editing the data is enabled/disabled
4. **Write:** Saving is enabled/disabled
5. **Print:** Printing is enabled/disabled
6. **Copy:** Copying is enabled/disabled

CONDITIONS

Conditions act as the expiration control of the license using various parameters that meet the software vendors' need

1. **Expiration Date:** A specific date specifies when the license should expire
2. **Expiration running time:** A specific value (minutes or hours) that specifies the exact effective duration the application/module should run.
3. **Expiration Period:** A specific value (days or months) that specifies the exact period the application/module should run.
4. **Max. No. of Trials:** A specific value that specifies how many times the application/module should run.
5. **Max. No. of Sessions:** A specific value that specifies how many sessions should be opened of the application/module. (used with Multi-user licenses)
6. **Max. No. of Users:** A specific value that specifies how many users should be accessing the application/module. (used with Multi-user licenses)

After issuing the license, the license file will be generated as .xml file. This xml file can be readable using any XML parser or Internet Explorer™. The following figure illustrates the readable license in Internet Explorer 6™



The license is characterized by being secure against alteration and modification; as it is based on PKI and Digital Signature techniques to secure the integrity of the license.

Executable Protection

E-Code Protection Studio v5.3.4 provides strong Executable (PE files) protection against reverse engineering and software cracking. This protection is called Safe Shell. The executable protection can be used as a standalone protection, or can be combined with Hardware Protection Technique. Mainly Exe protection provides the following

1. Protection against reverse engineering
2. Protection against debuggers
3. Protection against disassembling tools
4. Protection against decompiling tools
5. Protecting the Source Code and Data
6. Protecting the Intellectual property

Exe protection is offered with variable parameters that can increase the protection and security according to software vendors' need.

Protection Levels

The protection level provides the vendor to tune the level of protection according to the requirements for balancing security and the performance. Protection level depends mainly on the concept of Source code Interceptions, which modifies the application original source code and changes its original execution flow during run-time. Protection level has 3 levels

LOW LEVEL

There is no source code interception. It only depends on Source code Encryption, and Anti-debugging routines.

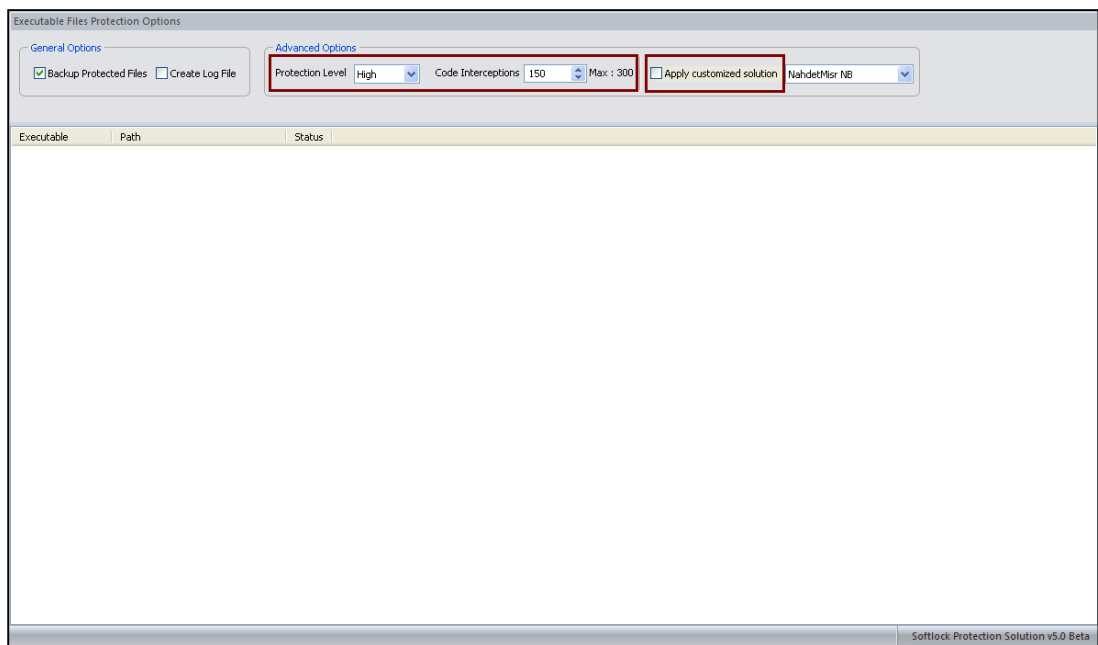
MEDIUM LEVEL

The number of Source code Interceptions varies from 50 to 100. The Anti-debugging routines are executed more often in run-time

HIGH LEVEL

The number of source code interceptions can reach 300. The Anti-debugging routines are executed extensively to detect debuggers.

Note: Increasing the Protection Level may decrease the performance of the running application.



Customized Protection Solutions

E-Code can provide a customized exe protection solution according to customer needs in order to meet all the protection requirements.

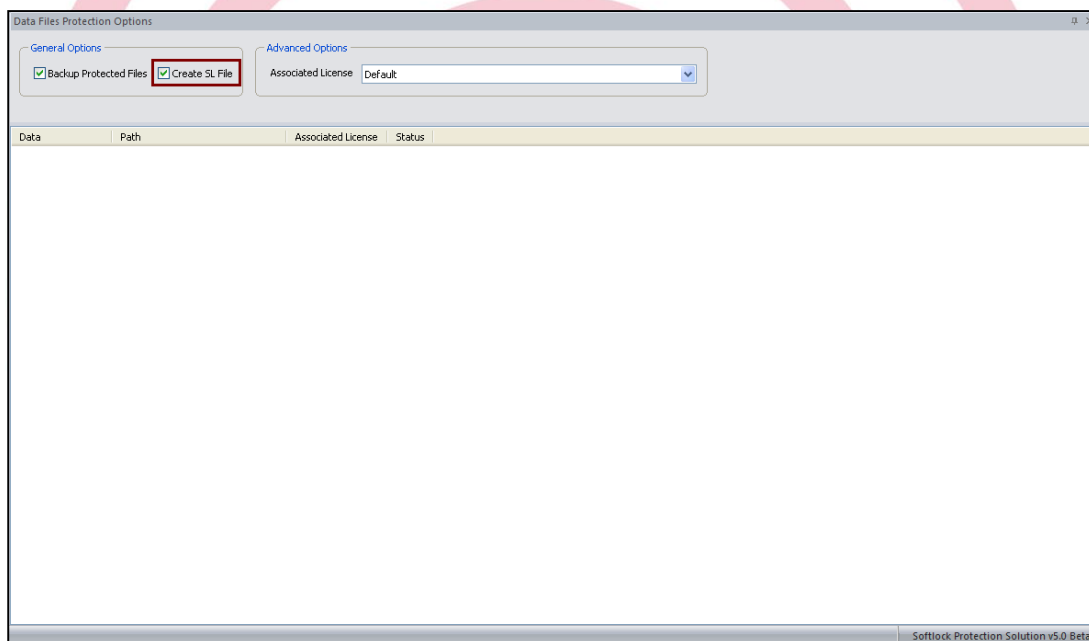
Data Files Encryption

E-Code Protection Studio provides strong data files encryption. Data protection technique is based on strong encryption technique (AES or 3DES), yet fast in run time operation. The data protection includes another level of protection during run-time for DRM.

The DRM applied to the data file is found in the license associated with it. This license is usually the license associated with the exe running the file.

Data Protection for R/W Files

Normally data file protection is applied to read only files. In order to apply it for R/W files it is required to generate (.SL) file beside the data file. Normally this option is suitable for protecting MS Access or SQL Lite database files.



Data file protection is combined with Safe Shell in order to provide Automatic Encryption/Decryption process during run-time. In this case, the protected Viewer/Reader of the file can read/write to the file in a transparent method, meanwhile the files cannot be illegally distributed without the License and combined hardware security.

Safe CD Protection

Safe CD protection is very popular in the field of protecting Multimedia, Games and small software. The purpose of this protection technique is in its low price and wide distribution through mass

production. E-Code Protection Studio v5.3.4 offers two versions of CD protection, which enables software vendors to choose the solution that best suits them.

CD STD

This version of CD protection is new in E-Code Protection Studio v5.3.4.

TECHNOLOGY

Safe CD STD depends on LS technology in protecting CDs. LS technology changes the physical characteristics of the output CD according to certain parameters generated by E-Code Protection Studio v5.3.4. Production of this CD protection depends on Machines that supports LS technology production using CD Stampers.

CHARACTERISTICS

Safe CD STD is characterized by:

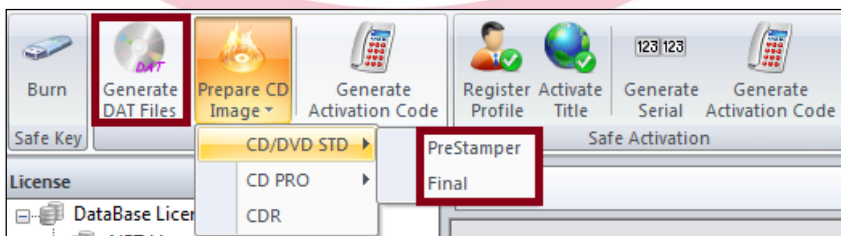
1. Faster CD Authentication during run-time
2. Various support for Old CD Drives

PROCESS

Safe CD STD production process is straight forward and easy. The following are the steps required for performing CD STD protection:

1. Create Title
2. Issue License with Safe CD/CDR protection type
3. Protect EXE + Encrypt Data (if required)
4. Generate DAT files according to remaining free size of the CD
5. Create a new image file for all the contents of the CD (Using any Image creator software)
6. Prepare the generated image using E-Code Protection Studio with CD STD
7. Burn the Image onto CD Stamper
8. Start replication of the CDs with a machine that supports LS technology

In case of preparing a PreStamper CD, in step 6, Prepare CD STD PreStamper. This PreStamper can be used in testing the protection before mass production using Final stamper.



CD PRO

This is an enhanced version of E-Code CD protection

TECHNOLOGY

Safe CD PRO depends on Physical Parameters Technology. This technology is considered one of the strongest technologies available for CD protection, as it changes physical parameters of the CD with strong and sensitive run-time authentication. CD stampers generated from this protection can be replicated using any CD machines.

CHARACTERISTICS

Safe CD PRO is characterized by:

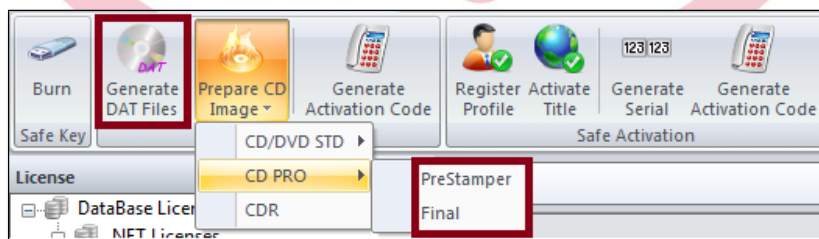
1. Strong and Secure Authentication method
2. Preparation process is faster than older version

PROCESS

Safe CD PRO production process is straight forward and easy. The following are the steps required for performing PRO protection:

1. Create Title
2. Issue License with Safe CD/CDR protection type
3. Protect EXE + Encrypt Data (if required)
4. Generate DAT files according to remaining free size of the CD
5. Create a new image file for all the contents of the CD (Using any Image creator software)
6. Prepare the generated image using E-Code Protection Studio with CD PRO
7. Burn the Image onto CD Stamper
8. Start replication of the CDs

In case of preparing a PreStamper CD, in step 6, Prepare CD PRO Pre-Stamper. This PreStamper can be used in testing the protection before mass production using Final stamper.



Safe CDR Protection

Safe CDR Protection is very popular in the field of protecting Multimedia, Games and small software. The purpose of this protection technique is in its low price and limited distribution. E-Code Protection Studio v5.3.4 provides Safe CDR Protection in order to meet many vendors requirements that is available in market.

Technology

Safe CDR depends on Special Signature Technology. This technology provides the strength for CDRs to prevent any illegal copy of the CDR contents.

Characteristics

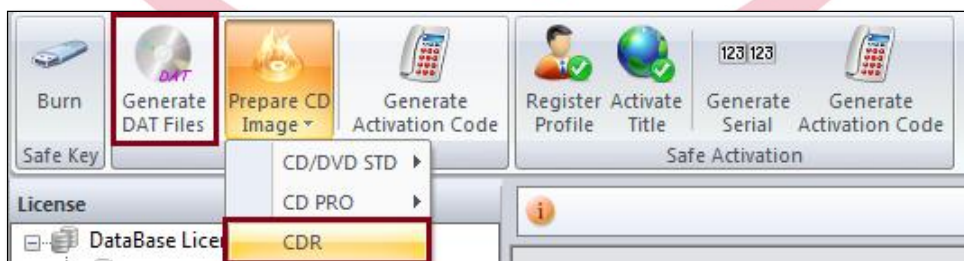
Safe CD version2 is characterized by:

1. Suitable for limited number of distribution
2. Prevents illegal contents copy
3. Fast Authentication method

Process

Safe CDR Production process is straight forward and easy. The following are the steps required for performing Safe CDR Protection:

1. Create Title
2. Issue License with Safe CD/CDR protection type
3. Protect EXE + Encrypt Data (if required)
4. Generate DAT files according to remaining free size of the CDR
5. Create a new image file for all the contents of the CDR (Using any Image creator software)
6. Prepare the generated image using E-Code Protection Studio with CDR
7. Start replication of the CDRs with machines supporting **Raw Mode**



Safe Key Protection

Safe Key protection is the new version of E-Code Dongle protection. Safe Key is offered in a new way to meet most vendors' requirements. Safe Key offers a strong protection that is considered hard to crack.

Technology

Safe Key protection technology is based over E-Code Smart Token. This protection depends on strong PKI standards that provide the maximum required protection. Safe Key protection provides user identification using Hardware Certificates that uniquely identifies the token.

Characteristics

Safe Key is characterized by:

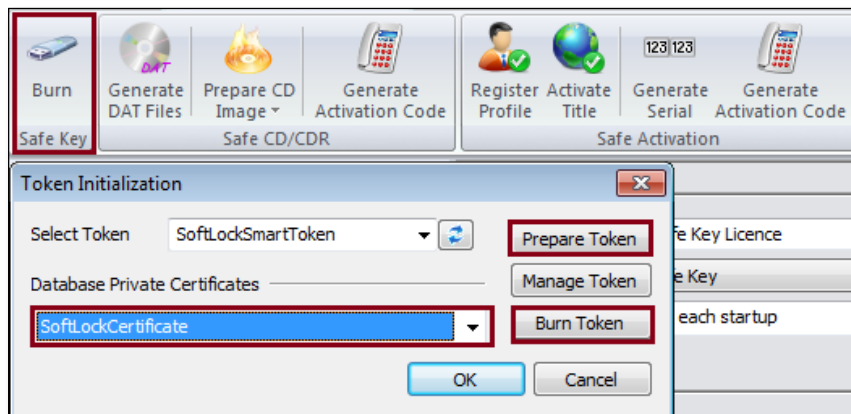
1. Driver-less USB device (USB HID device)
2. Based on PKI Standard
3. Offered in two models (Safe Key STD and Safe Key PRO)
4. Flexible License Management and Multi-User control
5. Flexible SDK API interface and features management

Process

Safe Key Production process is straight forward and easy. The following are the steps required for performing Safe Key Protection:

1. Create Title
2. Generate Certificate for User
3. Burn Certificate on Safe Key
4. Issue License with Safe Key protection type for the Burned Safe Key
5. Protect EXE + Encrypt Data (if required)

Safe Key provides flexible license options. Vendor can select Multi-User option (Server or Client) for generating a Network license that controls limited or un-limited number of users working on this license. Vendor can also prepare the tokens for the protection, so that it can be used only with his own protection titles.



Safe Activation Protection

Safe Activation protection is the new version of E-Code Online Activation protection. Safe Activation is offered in a new way to meet most vendors' requirements. Safe Activation offers a strong protection that is considered hard to crack.

Technology

Safe Activation protection technology is based over Online Internet Activation using web server. This protection depends on strong PKI standards that provide the maximum required protection. Safe Activation protection provides user identification using Machine Identification that uniquely identifies the user machine along with Unique Serials.

Characteristics

Safe Activation is characterized by:

1. Internet Online Activation and Administration control using Web Server
2. Unique Serials with multiple options (Multiple Machines Per Serial)
3. Flexible License Management and Multi-User control
4. Flexible SDK API interface and features management

Process

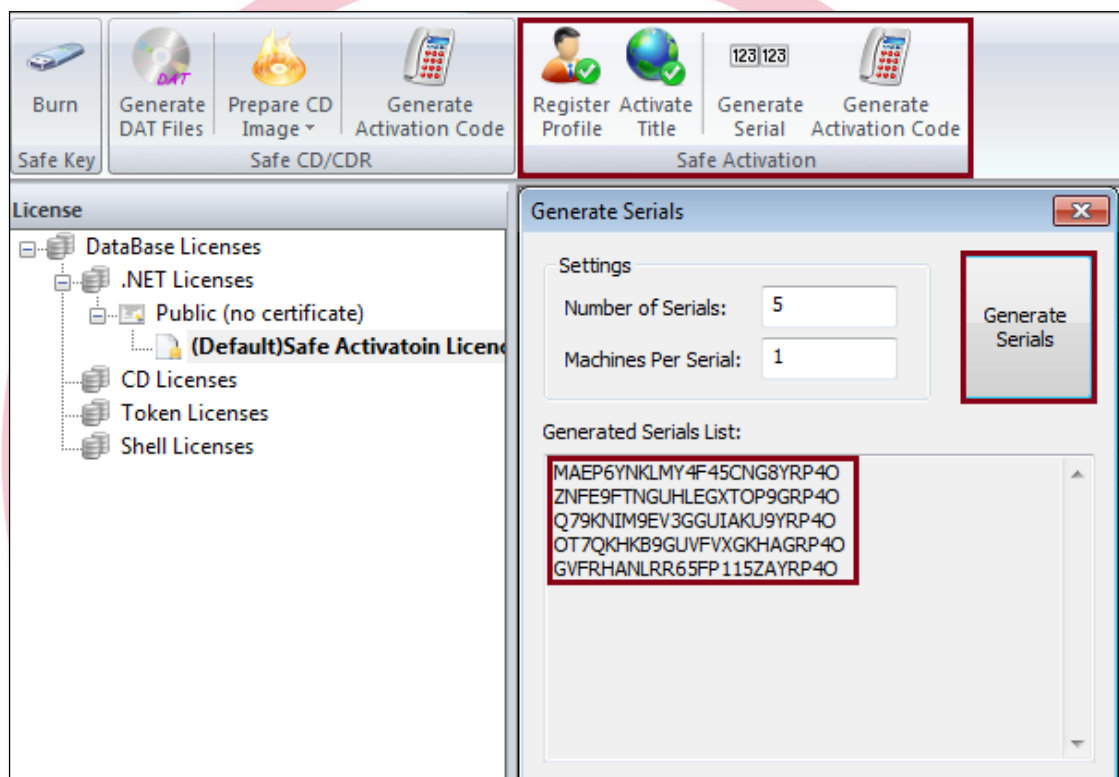
Safe Activation Production process is straight forward and easy. The following are the steps required for performing Safe Activation Protection:

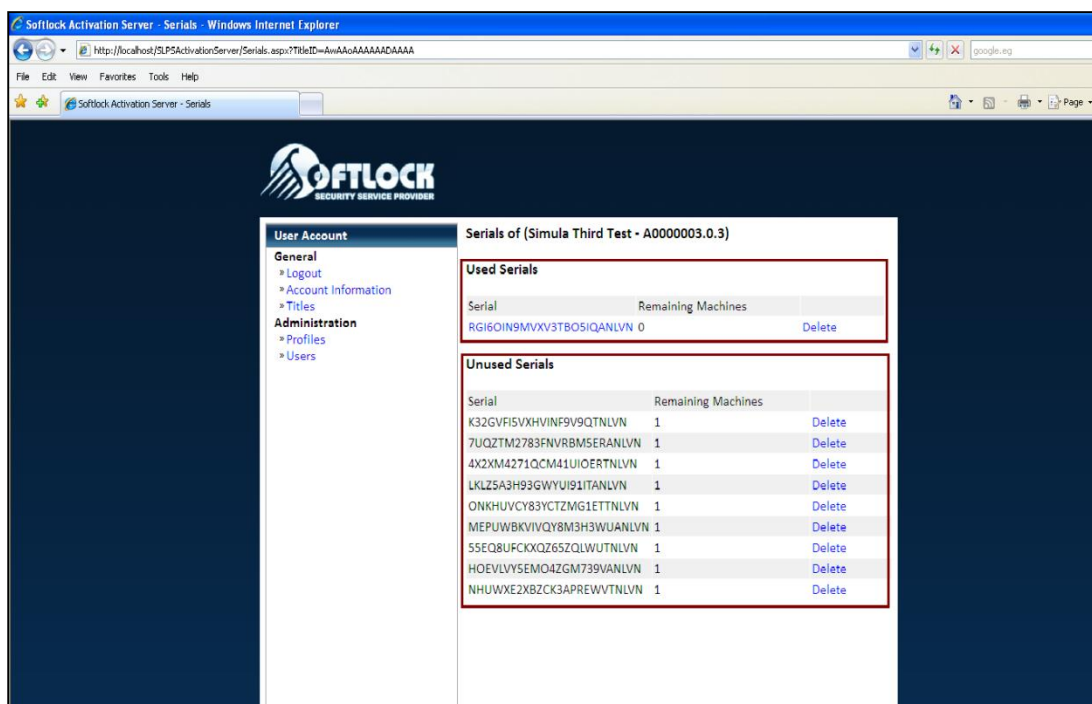
1. Create Title
2. Issue License with Safe Activation protection type (Public or Private license)
3. Protect EXE + Encrypt Data (if required)
4. Register Profile

5. Activate Title
6. Generate Serials with desired options

Safe Activation provides flexible license options. Vendor can select Multi-User option (Server or Client) for generating a Network license that controls limited or un-limited number of users working on this license. Vendor can host the Activation server on E-Code server or on premise.

Activation Web Server provides all the administration privilege for the vendor to control all the activated users and machines on the web server.





Software Protection Models

Safe Shell

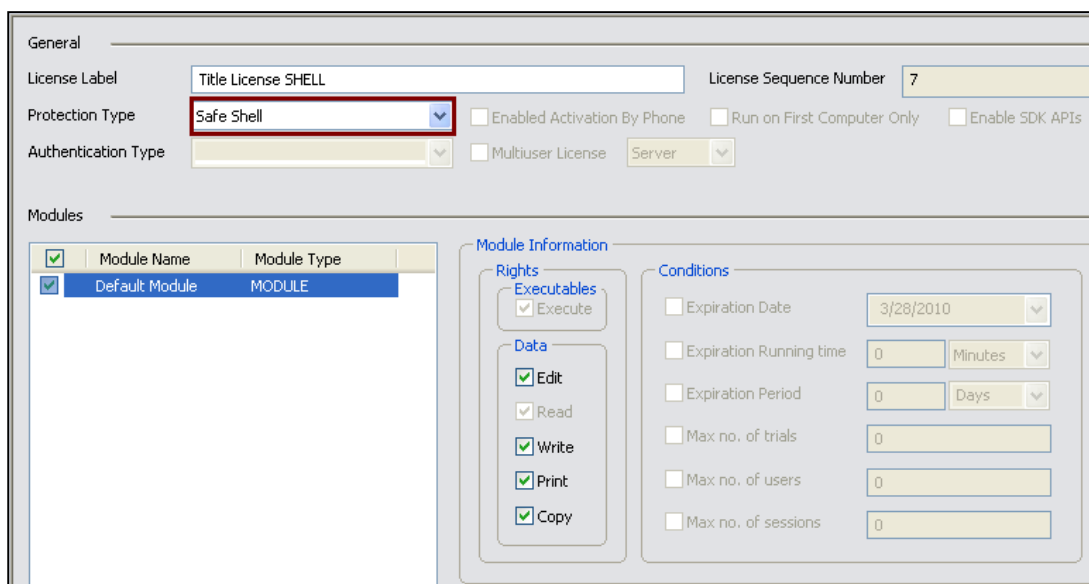
Safe Shell is the protection model for protecting the Exes without binding the protection to any hardware device. This kind of protection is useful for:

1. Protecting Intellectual Property
2. Protecting Data
3. Protection with low price; as it doesn't depend on any hardware device

Though, it doesn't support any license distribution control, and operate on a license with limited options. Safe Shell can be established with the following steps:

1. Create Title
2. Issue License with protection type: **Safe Shell**
3. Protect Exe
4. Encrypt Data (if required)

After distributing the software, The Software can run on any machine without any hardware authentication and activation. As shown in the following figure, no conditions or advanced license attributes are enabled in Safe Shell.



General

License Label: Title License SHELL License Sequence Number: 7

Protection Type: **Safe Shell** ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☐ Enable SDK APIs

Authentication Type: ☐ Multiuser License Server

Modules

Module Name	Module Type
Default Module	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☐ Expiration Date: 3/28/2010

☐ Expiration Running time: 0 Minutes

☐ Expiration Period: 0 Days

☐ Max no. of trials: 0

☐ Max no. of users: 0

☐ Max no. of sessions: 0

Safe Key with Single License and Single Key

In this model, the vendor will distribute each Safe Key with a unique single license. In this way, each user receives the Software package, should receive the Safe Key for activation with the License file corresponding to this key. This model is suitable for:

1. Distributing software while taking control over each user
2. Taking into consideration future license updates per user

The following steps describe how to use E-Code Protection Studio v5.3.4 to perform the mentioned license model:

1. Create Title
2. Generate **X** Certificates for **X** Users
3. Burn **X** Certificate on **X** Tokens (Safe Keys), as each user should have a unique Key
4. Issue **X** Licenses with the desired conditions with protection type: Safe Key, with License Certificate corresponding to each Safe Key (i.e. to each User)
5. Protect Exe + Data (if required)

This type of protection supports all license conditions and attributes. The following figure illustrates the different license options for Safe Key licenses.

General

License Label: Title License Key License Sequence Number: 7

Protection Type: Safe Key ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☐ Enable SDK APIs

Authentication Type: On each startup ☐ Multiuser License Server

Modules

Module Name	Module Type
Default Module	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit ☒ Read ☒ Write ☒ Print ☒ Copy

Conditions

☐ Expiration Date: 3/28/2010

☐ Expiration Running time: 0 Minutes

☐ Expiration Period: 0 Days

☒ Max no. of trials: 20

☐ Max no. of users: 0

☐ Max no. of sessions: 0

Safe Key with Single License and Multiple Keys

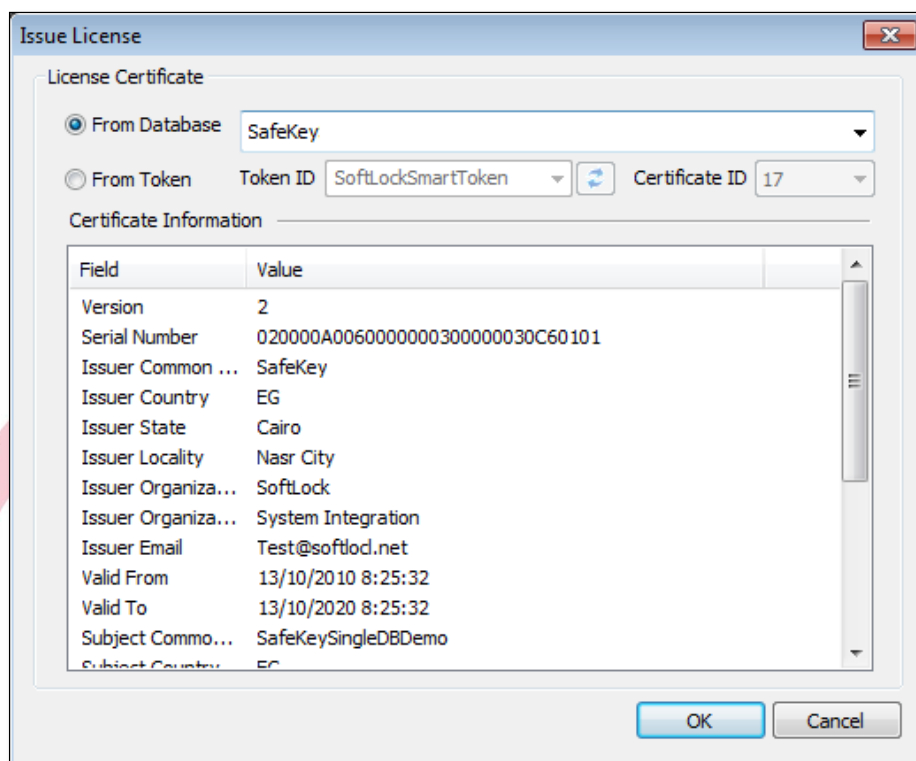
In this model, the vendor will distribute all Safe Key with a single license. In this way, a Single License file will be issued to multiple Users. This model is suitable for:

1. Distributing software for Multiple users without tracking their licenses
2. Future License updates will apply to all Users using a Single file
3. Less effort in Distribution and Production

The following steps describe how to use E-Code Protection Studio v5.3.4 to perform the mentioned license model:

1. Create Title
2. Generate 1 Certificate
3. Burn 1 Certificate on X Tokens (Safe Keys), as each user should have a unique Key
4. Issue 1 License with the desired conditions with protection type: Safe Key, with License Certificate that will be distributed to all Users
5. Protect Exe + Data (if required)

The following figure illustrates issuing the license for single certificate to be distributed with all Hardware Tokens



Safe Key with Multiple License and Single Key

In this model, the vendor will issue Multiple Licenses with different protection titles for a Single Safe Key. This model is suitable for:

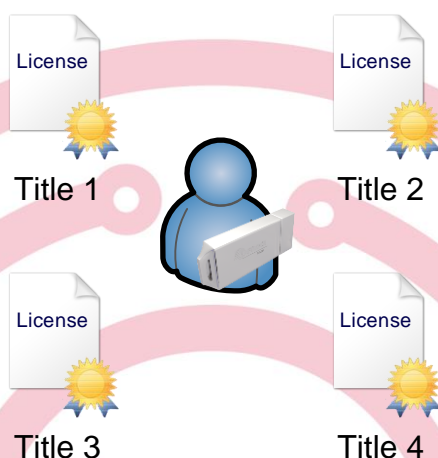
1. Distributing Multiple software for Single User
2. Decreasing the number of distributed Hardware Tokens
3. Less effort in Distribution and Production

The following steps describe how to use E-Code Protection Studio v5.3.4 to perform the mentioned license model:

1. Create Title
2. Generate **1** Certificate
3. Burn **1** Certificate on **1** Token (Safe Key), for single user
4. Issue **1** License with the desired conditions with protection type: Safe Key, with License Certificate that is corresponding to the user Token
5. Protect Exe + Data (if required)
6. Create **X** Titles
7. Issue **X** Licenses for **X** titles with the desired conditions with protection type: Safe Key, with License Certificate that is corresponding to the same user Token

8. Protect Exe + Data (if required)

The following figure illustrates how a Single hardware token, can run different applications from different titles.



Safe Key with Run on First Machine

In this model, the vendor will issue Safe Key license, with the limitation of running on the first machine the Safe Key activates on. This model is suitable for:

1. Distributing Safe Key and Binding to machine
2. Increased control on Software Distribution and Safe Key usage

The following steps describe how to use E-Code Protection Studio v5.3.4 to perform the mentioned license model:

1. Create Title
2. Generate **1 (or X)** Certificates
3. Burn **1 (or X)** Certificate on **1 (or X)** Token (Safe Key), for single **(or X)** user
4. Issue **1 (or X)** License with the desired conditions with protection type: Safe Key, and **Run On First Computer Only** option with License Certificate that is corresponding to the single **(or X)** user Token
5. Protect Exe + Data (if required)

Once the Safe Key has been distributed and the application ran once on the machine (i.e. Activating the Safe Key), the user cannot redistribute the software or reuse the Token on any other machine.

General

License Label: License Sequence Number:

Protection Type: ☐ Enabled Activation By Phone ☒ Run on First Computer Only ☐ Enable SDK APIs

Authentication Type: ☐ Multiuser License

Modules

<input checked="" type="checkbox"/>	Module Name	Module Type
<input checked="" type="checkbox"/>	Default Module	MODULE
<input checked="" type="checkbox"/>	Report Feature	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☐ Expiration Date:

☐ Expiration Running time: Minutes

☐ Expiration Period: Days

☐ Max no. of trials:

☐ Max no. of users:

☐ Max no. of sessions:

Software Licensing Models

Trial License

In this model, the vendor will issue a license for the protected software and data as a Trial license. E-Code Protection Studio v5.3.4 provides different conditions in order to meet these criteria. This model is suitable for:

1. Distributing license with Expiration Date
2. Distributing license with Number of Trials
3. Distributing license with Expiration Period (Number of Days/Months)

This model is available with the following protection techniques

1. Safe Key
2. Safe Activation

The following license has the following properties that can be very useful as a Trial License:

1. Issued for Safe Key protection
2. Expires on 30.04.2010
Or
3. Expires after 30 Days of its first run
Or
4. Expires after 40 Trials of the Software

The screenshot shows the 'General' tab of the E-Code Protection Studio v5.3.4 interface. The 'License Label' field contains 'SW2 F2 P0 License Key TRIAL' and the 'License Sequence Number' is '7'. The 'Protection Type' is set to 'Safe Key' (highlighted with a red box). The 'Authentication Type' is 'On each startup'. There are checkboxes for 'Enabled Activation By Phone', 'Run on First Computer Only', 'Enable SDK APIs', and 'Multiuser License'. The 'Modules' section shows a table with 'Default Module' and 'MODULE'. The 'Module Information' section has 'Rights' (Execute, Edit, Read, Write, Print, Copy) and 'Conditions' (Expiration Date: 4/30/2010, Expiration Running time: 0 Minutes, Expiration Period: 30 Days, Max no. of trials: 40, Max no. of users: 0, Max no. of sessions: 0). The 'Expiration Date', 'Expiration Period', and 'Max no. of trials' fields are highlighted with red boxes.

Note: Converting from Trial License to Final license can be easily established, and will be mentioned later.

Rental License

In this model, the vendor will protect the software and data using a license that can be used for renting the software, meanwhile providing flexible License Renewal model. E-Code Protection Studio v5.3.4 provides different conditions in order to meet these criteria. This model is suitable for:

1. Distributing license with Expiration Date
2. Distributing license with Expiration Running Time (Effective time in Minutes/Hours)
3. Distributing license with Expiration Period (Number of Days/Months)

Expiration Running Time: is the duration which the Software actually runs. For Example, a vendor can issue a license that can run effectively for 5 minutes.

This model is available with the following protection techniques

1. Safe Key
2. Safe Activation

The following license has the following properties that can be very useful as a Rental License:

1. Issued for Safe Key protection
2. Expires on 30.04.2010
Or
3. Expires after 30 Days of its first run
Or
4. Expires after 10 minutes of effective running

The screenshot displays the 'General' tab of the E-Code Protection Studio v5.3.4 interface. The 'License Label' field contains 'SW2 F2 P0 License Key RENTAL' and the 'License Sequence Number' is '7'. The 'Protection Type' is set to 'Safe Key', 'Authentication Type' is 'On each startup', and the 'License' is 'Server'. The 'Modules' section shows a table with 'Default Module' and 'MODULE'. The 'Module Information' section shows 'Rights' (Execute, Edit, Read, Write, Print, Copy) and 'Conditions' (Expiration Date: 4/30/2010, Expiration Running time: 10 Minutes, Expiration Period: 30 Days).

Note: License Renewal for a Rental License can be established using License Update model, and will be mentioned later.

Features License

In this model, the vendor will protect the software while applying license control on Special Parts of the software. E-Code Protection Studio v5.3.4 provides different conditions in order to meet these criteria. This model is suitable for:

1. Distributing license with control on Different Modules
2. Distributing license with Rental/Trial/Final conditions for each module

This model is available with the following protection techniques

1. Safe Key
2. Safe Activation

The following license has the following properties that can be very useful as a Features License:

1. Issued for Safe Key protection
2. Contains Two features (Modules): Reporting Feature and Accounting Feature
3. Accounting Feature is Disabled (not Checked)
4. Reporting Feature Expires on 30.04.2010
Or
5. Reporting Feature Expires after 30 Days of its first run of the feature
Or
6. Reporting Feature Expires after 10 minutes of effective running
Or
7. Reporting Feature Expires after 60 number of trials

General

License Label: SW2 F2 P0 License Key FEATURES License Sequence Number: 7

Protection Type: Safe Key ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☐ Enable SDK APIs

Authentication Type: On each startup ☐ Multiuser License Server

Modules

Module Name	Module Type
Default Module	MODULE
Reporting Feature	MODULE
Accounting Feature	MODULE

Module Information

Rights

Executables ☒ Execute

Data ☒ Edit ☒ Read ☒ Write ☒ Print ☒ Copy

Conditions

☒ Expiration Date: 4/30/2010

☒ Expiration Running time: 10 Minutes

☒ Expiration Period: 30 Days

☒ Max no. of trials: 60

☐ Max no. of users: 0

☐ Max no. of sessions: 0

Note: The shown conditions apply to Reporting Feature Only, while the Default Module contains the conditions applying to the whole Software. This model requires SDK development.

Network License

In this model, the vendor will protect the software controlled by a license placed in a network server. E-Code Protection Studio v5.3.4 provides different conditions in order to meet these criteria. This model is suitable for:

1. Single license controlling Multiple Users
2. Controlling Number of Users using the Software
3. Reducing the Hardware Activation and Distribution (Ex: Single Key runs Multiple Users)

This model is available with the following protection techniques

1. Safe Key
2. Safe Activation

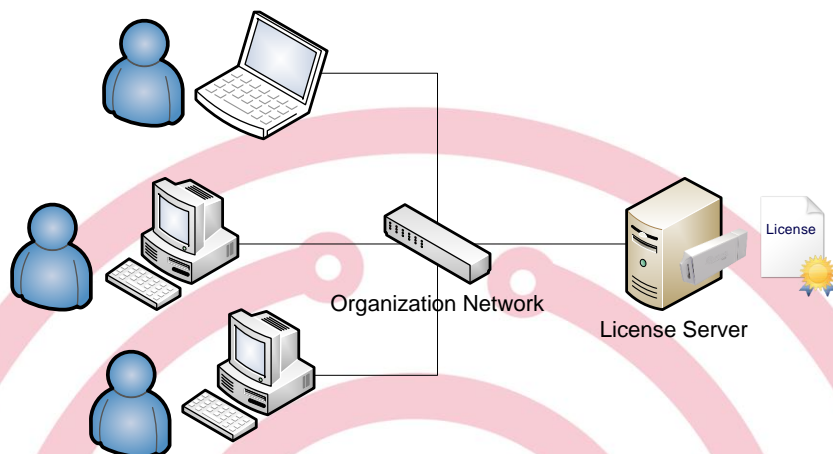
The following license has the following properties that can be very useful as a Network License:

1. Issued for Safe Key protection
2. Issued with Multi-User License and identified as Server License
3. Only 5 Users can run the software simultaneously

The screenshot shows the 'General' tab of the E-Code Protection Studio v5.3.4 license configuration window. The 'License Label' is 'SW2 F2 P0 License Key NETWORK' and the 'License Sequence Number' is '7'. The 'Protection Type' is 'Safe Key'. The 'Authentication Type' is 'On each startup'. The 'Multiuser License' checkbox is checked, and the 'Server' dropdown is selected. The 'Modules' section shows a table with 'Default Module' and 'MODULE'. The 'Module Information' section shows 'Rights' (Executables: Execute, Data: Edit, Read, Write, Print, Copy) and 'Conditions' (Expiration Date: 4/30/2010, Expiration Running time: 10 Minutes, Expiration Period: 1 Months, Max no. of trials: 0, Max no. of users: 5, Max no. of sessions: 0). The 'Max no. of users' field is highlighted with a red box.

Using a Server License requires installing E-Code Network Service on the License Server. In this model, the license can control the number of users running the software and the number of sessions the whole users can run on their machines simultaneously.

The Multi-User license can include any conditions that provide Trial or Rental licensing model. The next figure illustrates how multiple users running the applications on their machines while connecting single Safe Key and Network License to the server.



Note: This protection works only for a LAN.

Network/Portable License (Hybrid)

In this model, the vendor will protect the software controlled by a license placed in a network server, while providing the option for running as a portable license independent from the Server. E-Code Protection Studio v5.3.4 provides different conditions in order to meet these criteria. This model is suitable for:

1. Single Server license controlling Multiple Users
2. Controlling Number of Users using the Software
3. Reducing the Hardware Activation and Distribution (Ex: Single Key runs Multiple Users)
4. Enabling selected users to run the software when departed from the network.

This model is available with the following protection techniques

1. Safe Key
2. Safe Activation

In order to achieve this model, Software vendor will issue two licenses:

1. Network License: License placed on the Server License for multi-user license.
2. Client License: License placed with user that enables the user to run the application independent from the Network License.

The following license has the following properties that can be very useful as a Network License:

1. Issued for Safe Activation protection

2. Issued with Multi-User License and identified as Server License
3. Only 5 Users can run the software simultaneously in the network
4. Server License is issued as a Public License which must be activated on the License Server Machine using Internet Activation Server.

General

License Label: License Sequence Number:

Protection Type: ☒ Safe Activation ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☒ Enable SDK APIs

Authentication Type: ☐ On each startup ☒ Multiuser License ☐ Server

Modules

Module Name	Module Type
Default Module	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☐ Expiration Date:

☐ Expiration Running time: Minutes

☐ Expiration Period: Days

☐ Max no. of trials:

☒ Max no. of users:

☐ Max no. of sessions:

Issue License

License Type

Select License Type: ☐ Private License (With Certificate) ☒ Public License (Without Certificate)

License Certificate

☒ Server ☐ Default Certificate

User Machine Code:

☐ Register Updated License

☐ Export Certificate to file

Certificate Information

Field	Value
-------	-------

The following license has the following properties that can be very useful as a Client License:

1. Issued for Safe Activation protection
2. Issued with Multi-User License and identified as Client License
3. Client License is issued as a Public License which must be activated on the user machine using Internet Activation Server.

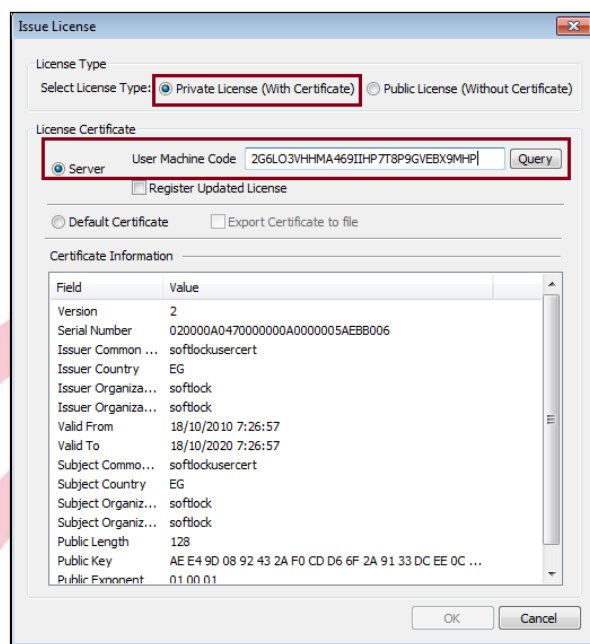
The screenshot shows the 'General' tab of a license configuration window. The 'License Label' is 'Test Title 1 License ACTIVATION Client' and the 'License Sequence Number' is '0'. The 'Protection Type' is set to 'Safe Activation' (highlighted with a red box). The 'Authentication Type' is 'On each startup'. The 'Multiuser License' checkbox is checked, and the 'Client' radio button is selected (both highlighted with a red box). The 'Modules' section shows a table with 'Default Module' and 'MODULE'. The 'Module Information' section includes 'Rights' (Execute, Edit, Read, Write, Print, Copy) and 'Conditions' (Expiration Date, Running time, Period, Max no. of trials, users, sessions).

Module Name	Module Type
Default Module	MODULE

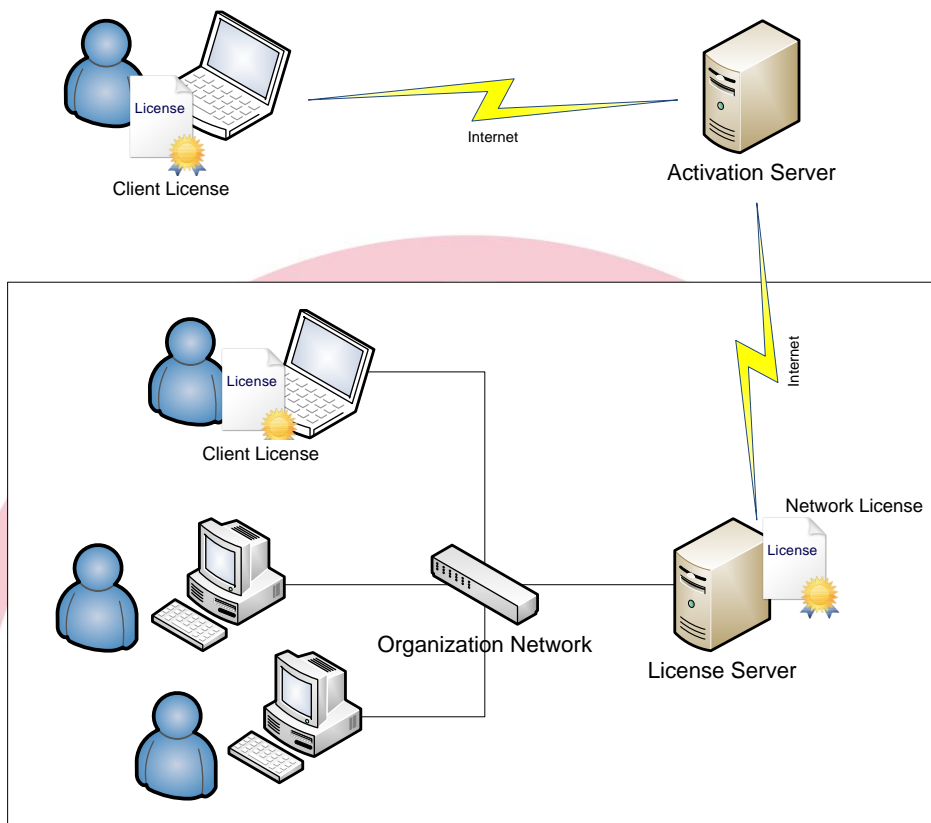
The Software will run according to the following constraints:

1. If Client Software is running in the network, then Network License will dominate and Client License will be ignored
2. If Client Software is running outside the network, then Client License will Activate using Internet Activation and ask the User for a Serial. This step is followed by issuing a Private License for the User Machine using License Update sequence.

The following figure illustrates issuing Private License for the Client License using Machine Code



The following figure illustrates the system of the Network/Portable license model. When the client license is running within the network, the Network license will dominate. While, when the Client License is departed from the network, it acts as a Portable license giving the ability for the user to run the software.



Note: This model can be applied to Safe Key protection, with the difference that the License Server will be activated by a Safe Key, and the User will run the portable license depending on another Safe Key owned by him. This model can be Protection technique independent, as the Network License can be Safe Activation, while Client License can be Safe Key (When Portable)

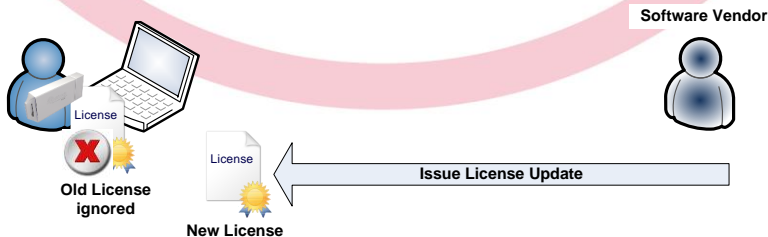
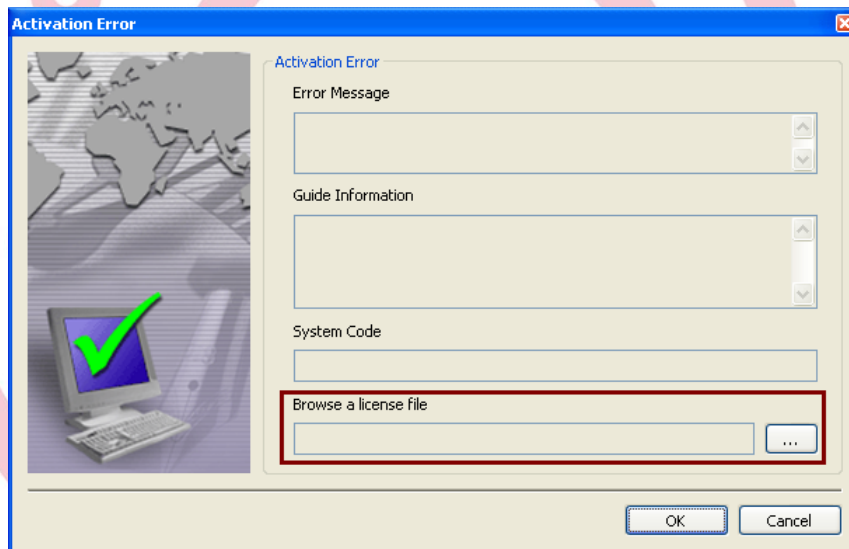
License Update

E-Code Protection Studio v5.3.4 provides a flexible license update model that fits different protection techniques.

Safe Key License Update

In this model, the vendor will update the License issued for a user running Software protected by Safe Key. The update process is done by the following steps:

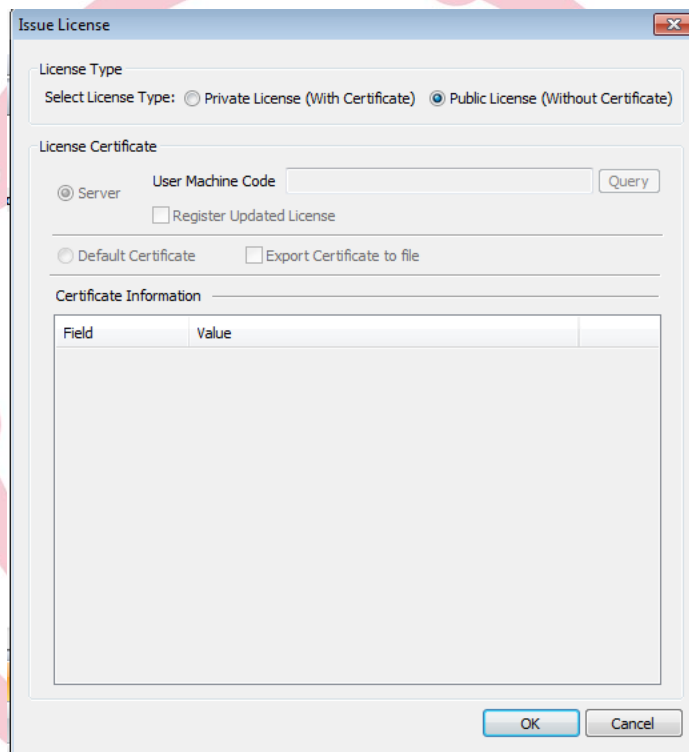
1. Open the old License, and Update the Rights and Conditions required for Update
2. Issue the New License for the Certificate burned on the Safe Key with the Target user
3. Send the License to the User
4. The User places the new License file in the same folder with the Exe
- Or
5. If the old license has been expired, user can use the Activation Error Dialog to browse the new license file.



Safe Activation License Update

In this model, the vendor will update the License issued for a user running Software protected by Safe Activation. The update process is done by the following steps:

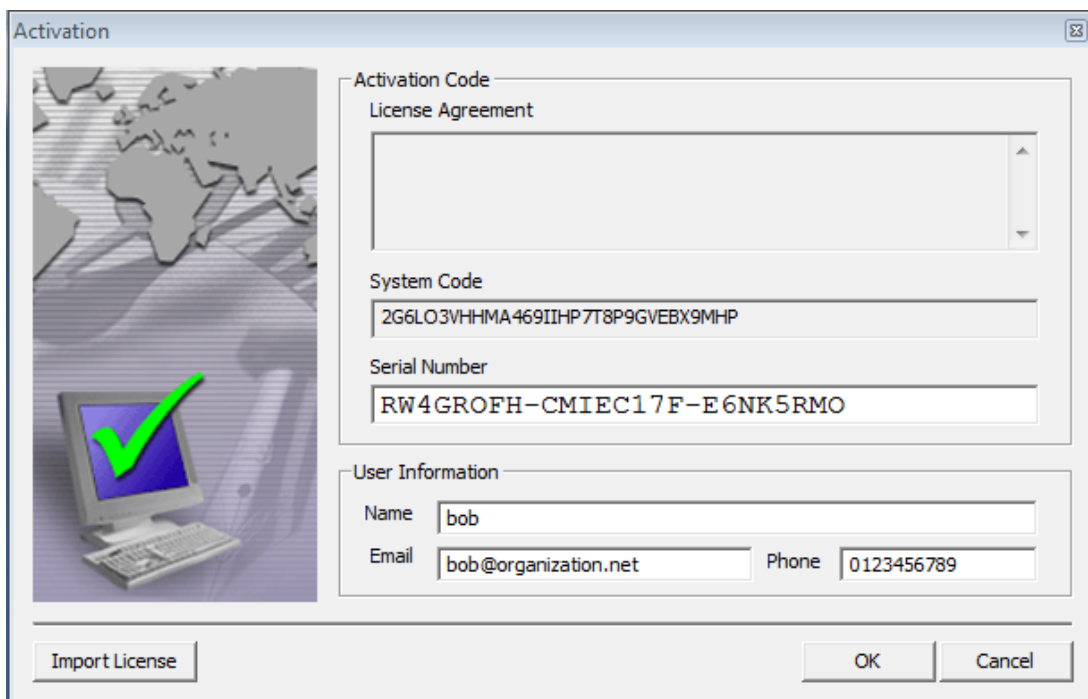
1. Vendor Issues Public License and Generate Serial
2. User Activate the Public License using the Serial
3. Vendor Issue a Private License using the User Machine Code
4. The User places the new License file in the same folder with the Exe
Or
5. If the old license has been expired, user can use the Activation Error Dialog to browse the new license file.



The Public License is issued so that it can run on any machine. The user activates the Public License using one of the Generated Serials. Generating Serials can be one of the following two models:

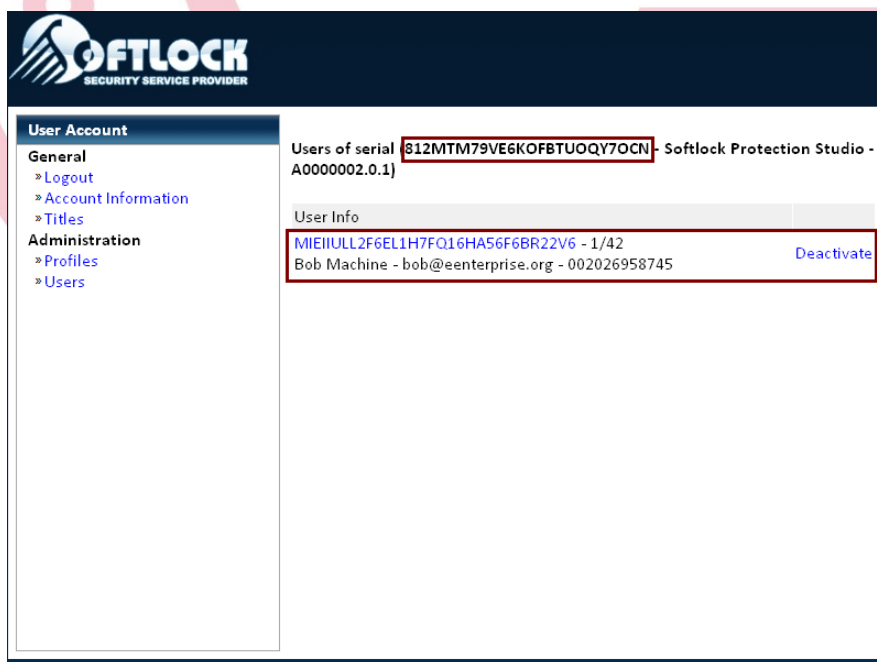
1. 1 Serial for Single Machine
2. 1 Serial for Multiple Machines

Once serial is used on the machine, the machine Code will be stored on the Activation server. The following figure illustrates Machine Activation using Serial.



The image shows a software activation dialog box titled "Activation". On the left is a graphic of a computer monitor with a large green checkmark. The main area contains three sections: "Activation Code" with a "License Agreement" text box; "System Code" with the value "2G6LO3VHHMA469IHP7T8P9GVEBX9MHP"; and "Serial Number" with the value "RW4GROFH-CMIEC17F-E6NK5RMO". Below these is the "User Information" section with fields for "Name" (bob), "Email" (bob@organization.net), and "Phone" (0123456789). At the bottom are buttons for "Import License", "OK", and "Cancel".

The following figure illustrates the Activation Server Web interface providing registered user activation information

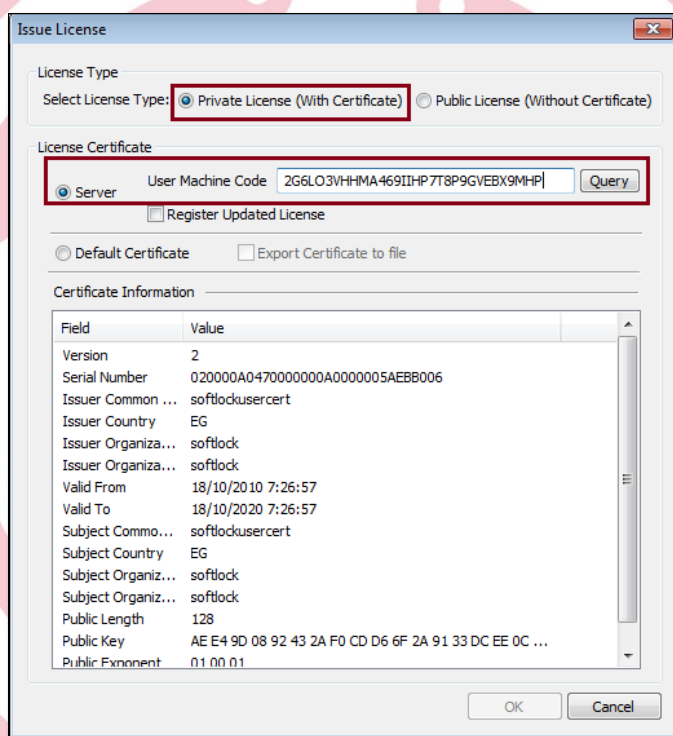


The image shows the Softlock Security Service Provider web interface. The header features the Softlock logo and the text "SECURITY SERVICE PROVIDER". The left sidebar contains a "User Account" menu with options: "General" (with sub-links "Logout", "Account Information", and "Titles"), and "Administration" (with sub-links "Profiles" and "Users"). The main content area displays information for a specific user account. It shows "Users of serial" followed by a red-bordered box containing the serial number "812MTM79VE6KOFBTUOQY7OCN", and "Softlock Protection Studio - A0000002.0.1)". Below this, the "User Info" section contains a red-bordered box with the text "MIEIUULL2F6EL1H7FQ16HA56F6BR22V6 - 1/42" and "Bob Machine - bob@eenterprise.org - 002026958745". A "Deactivate" link is visible to the right of the user info box.

In order to perform license update, Software vendor will issues a new license. The new License should be issued to specific user who requires a license update. This License is called a Private License. Private License can be issued using the following steps:

1. Vendor Selects a Private License option
2. Vendor types the User's Machine Code and click on Query
3. The User's private certificate will be retrieved from the Activation Server
4. The vendor can issue the Private License to the user.

The following figure illustrates issuing a Private License using Activation Server Query



Protection Techniques Migration

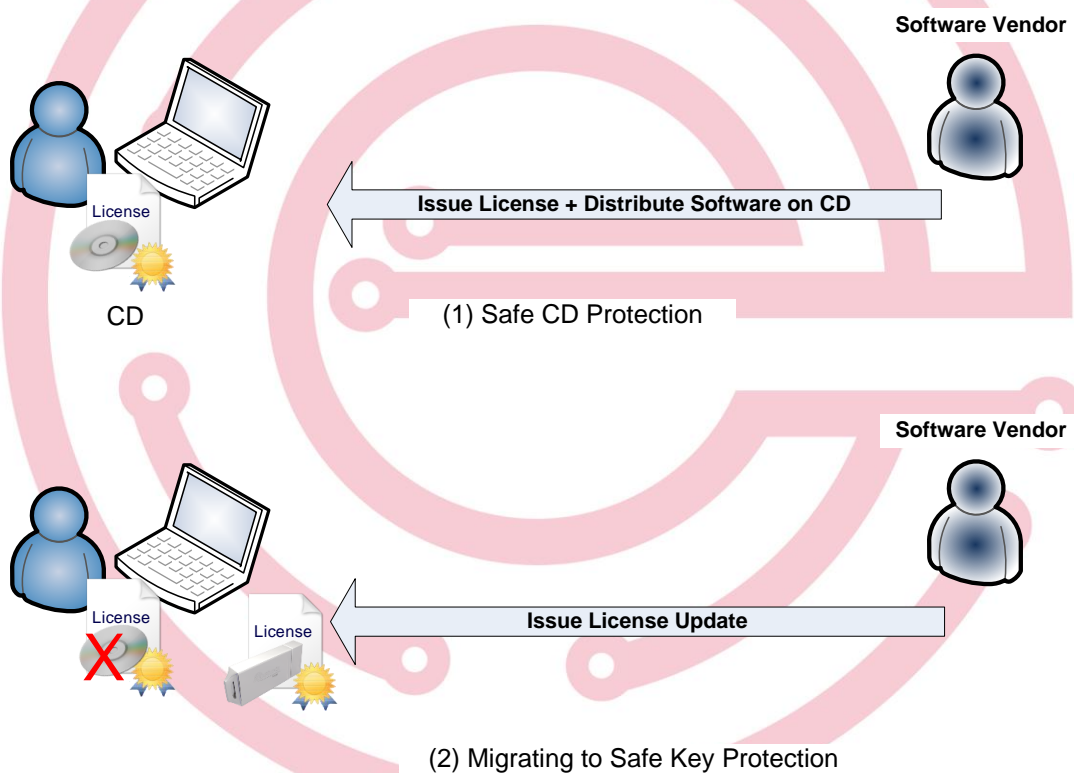
In this model, the vendor will be able to change the Protection Technique of the software without the requirement of going through the whole Application and Data protection process. The protection technique migration depends on the license update operation. The protection technique process is done by the following steps (Migrating from CD to Safe Key):

1. Vendor starts protecting the application and data
2. Vendor issues a license with CD protection type

3. Vendor prepares the NRG image, replicate and distribute the CDs

The following steps illustrates the migration to Safe Key protection

1. Vendor uses the same title of the protected CD application
2. Vendor generates a Certificate for the user, Prepare a Safe Key, and Burn the certificate on the Key
3. Vendor issues a new license (License Update) with Safe Key protection type, issued for the user's key
4. User places the new License in the same folder with the protected application, plugs the Safe Key and runs the application, and then the application automatically starts to work as a Safe Key protected application.



Offline Activation (Phone)

E-Code Protection Studio v5.3.4 provides a flexible Offline Activation operation, which has a great benefit for Safe CD and Safe Activation protection techniques. Offline Activation is an option used in the case of physical authentication failure, whether authenticating to protected CD or Activation Server via internet.

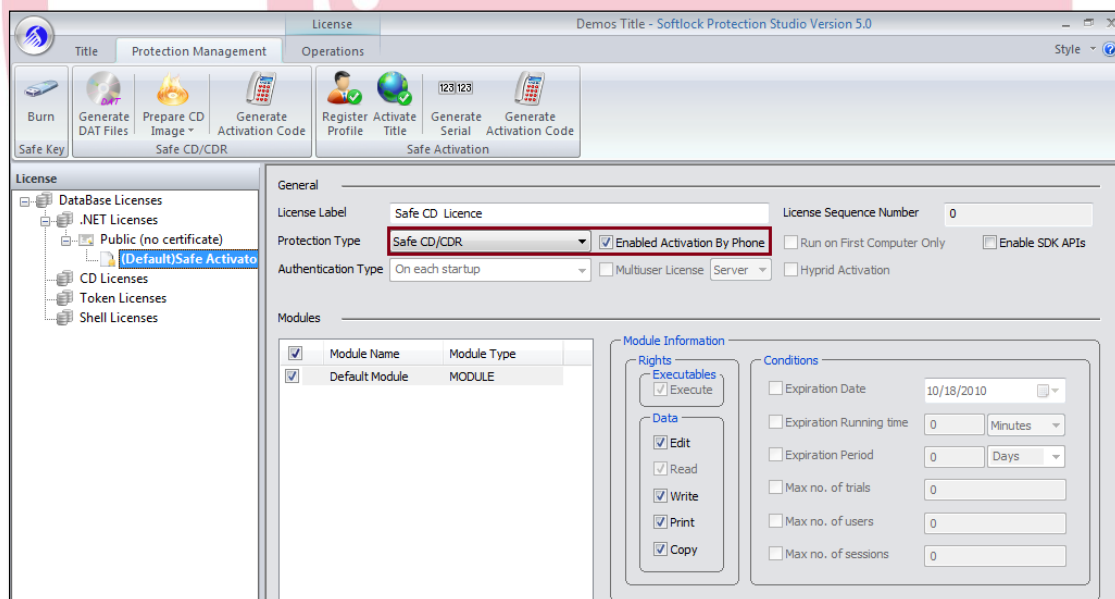
Safe CD with Offline Activation

In this model, the vendor will be able to activate the software even though the CD authentication has failed due to any reason. The protection technique process is done by the following steps:

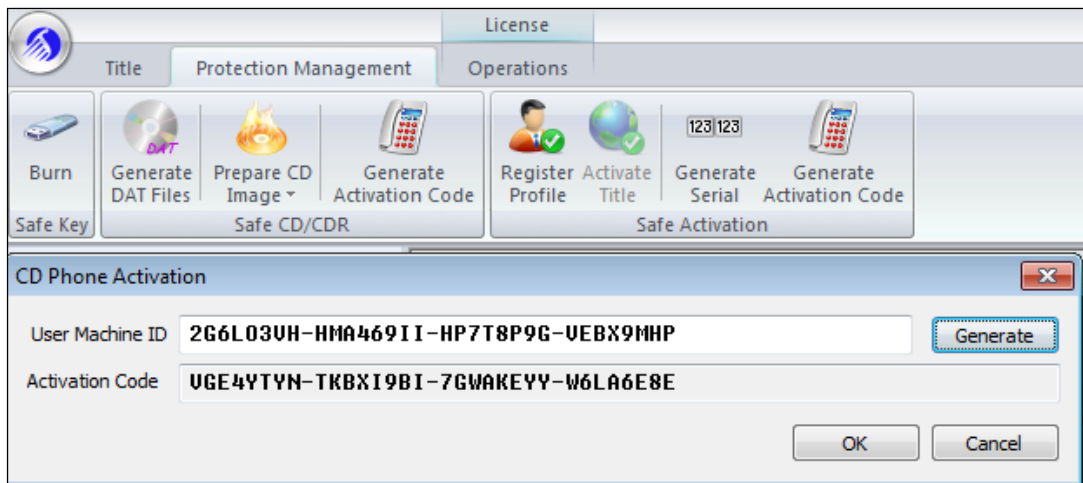
1. Vendor starts protecting the application and data
2. Vendor issues a license with CD protection type and with Enable Phone Activation
3. Vendor prepares the NRG image, replicate and distribute the CDs

If one of the users' CD failed to activate

1. Vendor gets the System Code from the user (in the Error Message)
2. Vendor enters the System Code in the User Machine ID field from Generate Activation Code
3. Vendor clicks on Generate, and Send the resulting Unique Activation Code to the user



The following figure illustrates the Activation Code Generation



Safe Activation with Offline Activation

In this model, the vendor will be able to activate the software even though the Safe Activation authentication has failed due to any reason. The protection technique process is done by the following steps:

1. Vendor starts protecting the application and data
2. Vendor issues a license with Safe Activation protection type and with Enable Phone Activation
3. Vendor Activate the Title, Generate Serials and distribute the software

If one of the users' application failed to activate

1. Vendor gets the System Code from the user (in the Error Message), Serial and user Info
2. Vendor enters the User Info, Serial and System Code in the System Code field from Generate Activation Code
3. Vendor clicks on Generate, and Send the resulting Unique Activation Code to the user

The generated Activation Code will be unique and represents the user. All the user info will be sent to activation server and the serial will be flagged as used.

The screenshot shows the 'Phone Activation' dialog box. It contains the following fields and values:

- User Name: Bob
- User Email: Bob@entrprise.com
- User Phone: 0123456789
- System Code: 2G6L03UH-HMA469II-HP7T8P9G-UEBX9MHP
- Serial Number: 9T5KYIQ8-HR7E4633-RKXY7RC0
- Activation Code: PRKK731X-OTI6IQGM-RKECG7TW-H2GQPBLW (highlighted with a red box)

Buttons include 'Generate', 'OK', and 'Cancel'.

The following figure illustrates the user info registered on the server after offline activation process

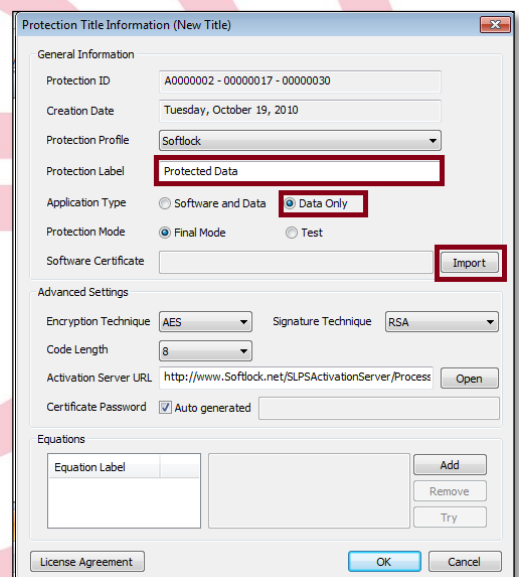
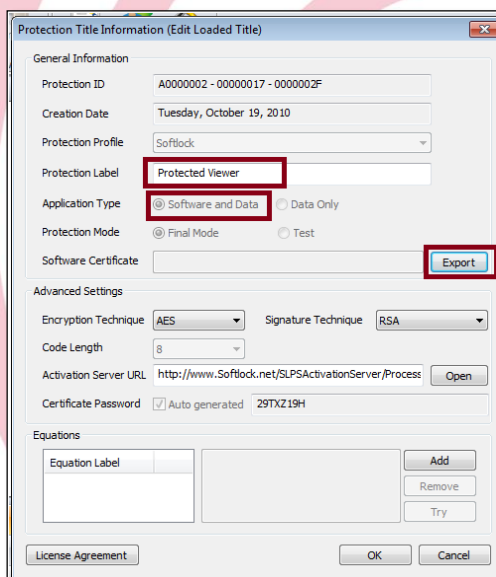
The screenshot shows the 'User Account' management interface for 'SOFTLOCK SECURITY SERVICE PROVIDER'. The left sidebar shows a navigation menu with 'General' selected. The main area displays 'Users of serial CHIVEK7WYL2516BO5N1GUCN - Test - A0000002.2.5'.

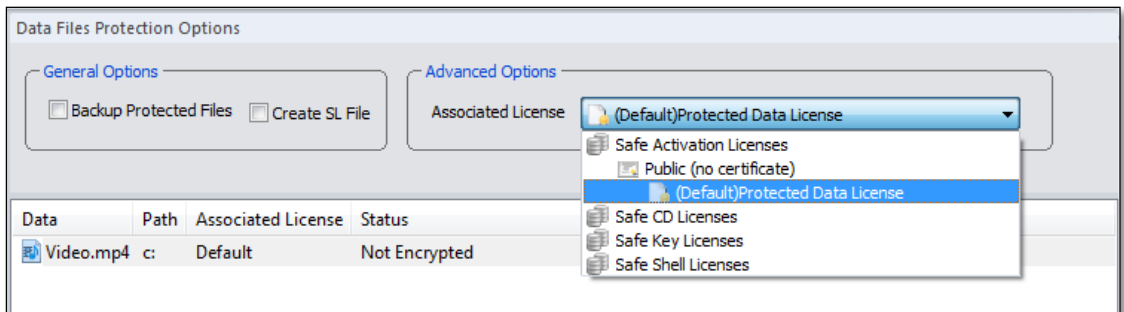
User Info	Activation Date	
dnojndfo - 0/0	5/16/2010	
bob stevenson - bob@eenterprise.org - 568232214	12:24:57 PM	Deactivate

Data Only Protection

In this type of applications the vendor who Produce Data like multimedia, videos, e-books and etc will be able to protect his products. The vendor develops a viewer which can be used to run the vendor's data. The protection technique process is done by the following steps:

1. The viewer will be protected using shell protection technique under software and data application type.
2. SW certificate of the Protected viewer will be exported
3. When the data only applications are protected using one of the protection techniques, the vendor has to use the SW certificate of the viewer in order to the viewer can view the protected data.
4. When the data is encrypted, the license will be appended at the end of the encrypted data.





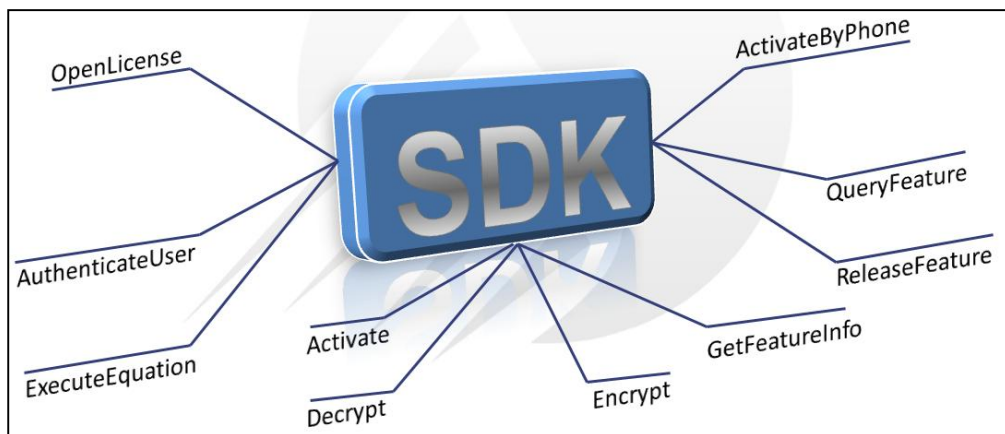
Protection with SDK

E-Code Protection Studio v5.3.4 provides a flexible SDK solution for developers. The SDK provides different APIs that gives the ability to the developer to extend the software protection.

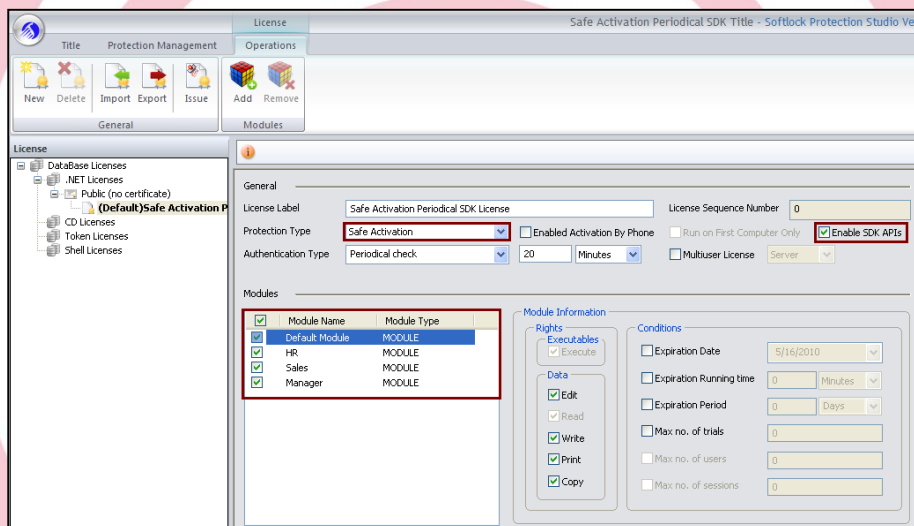
Using SDK, the vendor will be able to extend the protection of the software by controlling different features in the software. SDK with modules is the method to apply protection to different parts of the software independently. E-Code Protection Studio APIs provide the needed functionalities to the developer to control different protected software features. The protection technique process is done by the following steps (works only for Safe Key and Safe Activation):

1. Vendor starts protecting the application and data
2. Vendor creates a license with Safe Activation protection type and with Enable SDK
3. Vendor adds different modules in the license, for example:
 - a. HR Module
 - b. Sales Module
 - c. Manager Module
4. Vendor specifies the rights and conditions for each module independently
5. Vendor issues the license and distribute the software
6. Vendor can issue license updates with new conditions and modules in the software if needed
7. Vendor should add the required source code in the development environment (ex: C++, C#, VB ...) which uses the E-Code Protection Solution SDK (SLPSSDK.dll) to take full control over the software features using the modules stored in the license.

The following figure illustrates sample of different APIs provided by SLPSSDK.dll



The following figure illustrates the license options for a SDK Enabled License



The following figure illustrates the conditions applied to HR Modules

1. Expires on 01/08/20101

General

License Label: Safe Activation Periodical SDK License License Sequence Number: 0

Protection Type: Safe Activation ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☒ Enable SDK APIs

Authentication Type: Periodical check 20 Minutes ☐ Multiuser License Server

Modules

Module Name	Module Type
<input checked="" type="checkbox"/> Default Module	MODULE
<input checked="" type="checkbox"/> HR	MODULE
<input checked="" type="checkbox"/> Sales	MODULE
<input checked="" type="checkbox"/> Manager	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☒ Expiration Date 8/1/2010

☐ Expiration Running time 0 Minutes

☐ Expiration Period 0 Days

☐ Max no. of trials 0

☐ Max no. of users 0

☐ Max no. of sessions 0

The following figure illustrates the conditions applied to **Sales Module**

1. Expires after 1 month from its first try
- Or
2. If Number of trials reached 30

General

License Label: Safe Activation Periodical SDK License License Sequence Number: 0

Protection Type: Safe Activation ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☒ Enable SDK APIs

Authentication Type: Periodical check 20 Minutes ☐ Multiuser License Server

Modules

Module Name	Module Type
<input checked="" type="checkbox"/> Default Module	MODULE
<input checked="" type="checkbox"/> HR	MODULE
<input checked="" type="checkbox"/> Sales	MODULE
<input type="checkbox"/> Manager	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☐ Expiration Date 5/16/2010

☐ Expiration Running time 0 Minutes

☒ Expiration Period 1 Months

☒ Max no. of trials 30

☐ Max no. of users 0

☐ Max no. of sessions 0

The following figure illustrates the conditions applied to **Manager Module**

1. The Manager module is not enabled, as it is not checked (Note that Execute Right is disabled as well)

General

License Label: Safe Activation Periodical SDK License License Sequence Number: 0

Protection Type: Safe Activation ☐ Enabled Activation By Phone ☐ Run on First Computer Only ☒ Enable SDK APIs

Authentication Type: Periodical check 20 Minutes ☐ Multiuser License Server

Modules

Module Name	Module Type
<input checked="" type="checkbox"/> Default Module	MODULE
<input checked="" type="checkbox"/> HR	MODULE
<input checked="" type="checkbox"/> Sales	MODULE
<input type="checkbox"/> Manager	MODULE

Module Information

Rights

Executables

☒ Execute

Data

☒ Edit

☒ Read

☒ Write

☒ Print

☒ Copy

Conditions

☐ Expiration Date: 5/16/2010

☐ Expiration Running time: 0 Minutes

☐ Expiration Period: 0 Days

☐ Max no. of trials: 20

☐ Max no. of users: 0

☐ Max no. of sessions: 0

The following figure illustrates SDK source code snippet written in C++, and checking on **HR Module**. The following are the APIs used in this source code snippet

1. SLPSOpenLicense
2. SLPSAuthenticateUser
3. SLPSActivate
4. SLPSGetLicenseGrants
5. SLPSQueryFeature

```
{
    unsigned int ERR;
    //Open the selected license
    ERR = SLPSOpenLicense(LicenseFileName, NULL, 0, licenseDlg.m_ProtectionID, SWCertificatePWD,
        licenseDlg.m_SWCertificatePWD.GetLength(), &m_hLicenseHandle);
    if(ERR != SLPS_OK) return ERR;

    //Authenticate the user
    ERR = SLPSAuthenticateUser(m_hLicenseHandle, TRUE);
    if(ERR != SLPS_OK) return ERR;

    //Activate the application
    ERR = SLPSActivate(m_hLicenseHandle);
    if(ERR != SLPS_OK) return ERR;

    //Get License Grants
    SSLPSGrantMap grantArray[20];
    unsigned int grantArrayCount=20;
    ERR = SLPSGetLicenseGrants(m_hLicenseHandle, grantArray, &grantArrayCount);

    //Query feature (Check if Exists and no condition violation occurred)
    unsigned int grantID = get_grant_number("HR");
    DWORD ERR = SLPSQueryFeature(m_hLicenseHandle, grantID, 1);
    if(ERR != SLPS_OK) return ERR;
}
```

V. PROTECTION SAMPLES

This section describes E-Code Protection Samples for E-Code Protection Studio v5.3.4.0

Safe CD/CDR Sample

Safe CD/CDR sample provides a simple illustration for CD/CDR protection. The sample is available in 3 NRG files for:

1. CD STD
2. CD PRO
3. CDR

In order to try the sample, the user should burn the NRG images to CD/CDR and try the protection. Please refer to user manual for detailed steps in preparing the protected CD/CDR.

Safe CD/CDR provides a clear example for CD/CDR copy protection and data protection. The sample displays number of Encrypted Macromedia Flash™ files (.swf) which cannot be displayed without the protected flash application.



Safe Activation Sample

Safe Activation sample provides a simple illustration for Internet Activation protection. The authentication type available for Safe Activation samples are:

1. Periodical Check: Where all the grants are stored on the Activation Server
2. Phone Enabled (Offline)

Safe Activation sample also provides a clear sample for Automatic Data Encryption/Decryption. The encrypted data includes:

1. SLPS.GIF: Image appears in the sample
2. Database.mdb: MS Access data base, where the protected sample performs Read/Write operations

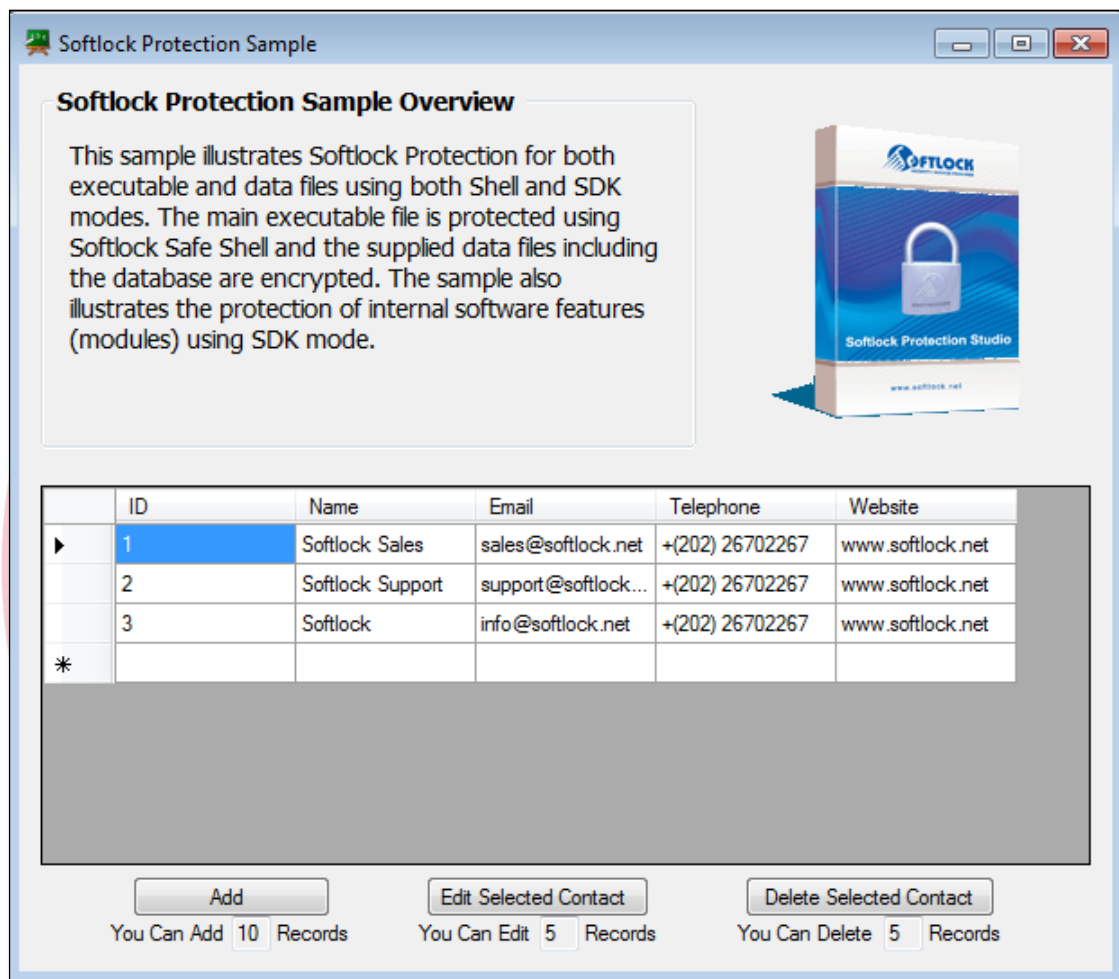
Safe Activation also provides a clear example for Software Features (Modules) protection. The protected modules (using SDK) are:

1. Add module: Adding new records to the database. The limitation is on the number of records to be added
2. Delete module: Deleting records from the database. The limitation is on the number of records to be deleted
3. Edit module: Editing records from the database. The limitation is on the number of records to be edited

```
- <grant>
  <KeyHolder licensePartIdRef="User Public Key" />
  <execute />
  <read />
  <write />
  <edit />
  <copy />
  <print />
- <ProtectedObject>
  <SWKey licensePartIdRef="SW Key" />
  <ProtectedObjectName>Delete</ProtectedObjectName>
  <ProtectedObjectType>Module</ProtectedObjectType>
</ProtectedObject>
  <MaxNumberOfTrials>5</MaxNumberOfTrials>
  <GrantID>1</GrantID>
</grant>
+ <grant>
  <KeyHolder licensePartIdRef="User Public Key" />
  <execute />
  <read />
  <write />
  <edit />
  <copy />
  <print />
- <ProtectedObject>
  <SWKey licensePartIdRef="SW Key" />
  <ProtectedObjectName>Add</ProtectedObjectName>
  <ProtectedObjectType>Module</ProtectedObjectType>
</ProtectedObject>
  <MaxNumberOfTrials>10</MaxNumberOfTrials>
  <GrantID>2</GrantID>
</grant>
+ <grant>
```


The figure illustrates part of the license associated with the sample.

The following figure illustrates the Safe Activation sample application indicating the encrypted GIF image and the different software features controlled by the license



Safe Key Sample

Safe Key sample provides a simple illustration for USB Dongle/Token protection. The authentication type available for Safe Key samples are:

1. Periodical Check: checking for the existing of the USB key with certain time interval.
2. Multi-User License: a sample with Server License and Multi-user control.

Safe Key sample is the same as Safe Activation sample, provides a clear sample for Automatic Data Encryption/Decryption. The encrypted data includes:

1. SLPS.GIF: Image appears in the sample
2. Database.mdb: MS Access data base, where the protected sample performs Read/Write operations

Safe Key also provides a clear example for Software Features (Modules) protection. The protected modules (using SDK) are:

1. Add module: Adding new records to the database. The limitation is on the number of records to be added
2. Delete module: Deleting records from the database. The limitation is on the number of records to be deleted
3. Edit module: Editing records from the database. The limitation is on the number of records to be edited

The Multi-user sample will require installing E-Code Protection Solution Network Service and installing the Server License on the server along with the USB Key.

VI. SPECIFICATIONS

E-Code Protection Studio v5.3.4

Supported Operating System	Windows 2K, XP, 2003, Vista, 7, 2008
License Activation	Available in Two Modes <ol style="list-style-type: none"> 1. Safe KEY protected Protection Studio 2. Safe ACTIVATION protected Protection Studio (Requires Internet connection)
Protection Techniques	Safe SHELL, Safe CD/CDR, Safe KEY and Safe ACTIVATION support. Controlled by Protection Studio License
Software Interface	SDK Library and SDK COM
Supported Standards	XrML
Cryptography	AES, 3DES, RSA

Safe CD/CDR

Supported Operating System	Windows 2K, XP, 2003, Vista, 7, 2008
Production	<ol style="list-style-type: none"> 1. CD Replication based on CD Stampers 2. CDR Replication based on regular CD Writers and Replicators with raw write mode
CD Protection Techniques	CD STD and PRO
CD Drive Interface Support	IDE

Safe Key

Supported Operating System	Windows 2K, XP, 2003, Vista, 7, 2008 and Linux
Hardware Interface	Plug and Play USB/HID. No driver is required.
Software Interface	PKCS, CSP, SDK library and SDK COM
Supported Standards	PKCS (1, 5, 7, 8, 10, 11 2.2 and 12), X5.09, CSP and FIPS 14-2-L2
Onboard Cryptography	RSA-1024 Signature , 3DES and AES
Operating Temperature Range	-25° to 85° C
Memory Retention	10000 write cycle and 10 years data retention

Safe Activation

Supported Operating System	Windows 2K, XP, 2003, Vista, 7, 2008 and Linux
Server IIS	IIS 5,6,7
Activation Server Vendor Interface	Admin Web page providing the vendor with full control of machine activation and serials control
Internet Secure Communication	RSA-1024, 3DES and AES
Server Hosting	On E-Code server or Vendor proprietary Server

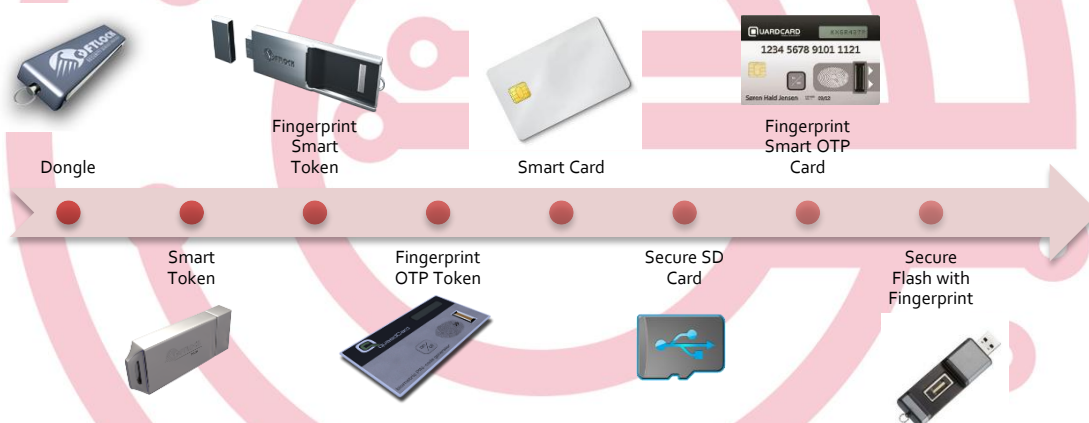
I. ABOUT E-CODE

E-Code is a leading progressive, innovative company in the field of information **security** providing **technology, state of the art solutions**, consulting, **integration and testing** services to safeguard the information assets, identities and the supporting infrastructure against unauthorized use.

Our high quality service and excellent benefits and the ability of being reliable and responsible put us as a leader on the top of digital security companies.

E-Code provides unique products and solutions, which cover many security areas fulfilling customers need in different market sectors. We provide a set of products and solutions covering the following areas: software protection, data encryption, security hardware, digital signature, secure identification and authentication, secure online distribution of digital Contents.

We supports different market sectors like; governmental institutes, organizations, banks, software development companies, multimedia software and game producers, media and eBooks publishers and individual users.



Website

www.e-code.com

Email

info@e-code.com, support@e-code.com, sales@e-code.com

Telephone

Fax

